EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: Axio Information Security Policy

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor _____will __X___ will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the

incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

Daniel Hirt

Signature

Daniel Hirt

Printed Name

Chief Operating Officer

Title

04/14/2021

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND AXIO GLOBAL, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Axio Global, Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Axio360 NY Education RIC Edition

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: Compliance with Axio Information Security Policy

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on April 15, 2021 and expires on June 30, 2024.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.

- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

Information Security Policy

Written by Audit Liaison

and Edited by Dan Hirt, COO

Version 1.4

January 2020

Table of Contents

Axio Information Security Management Policy and Procedures

Purpose:	This policy, consisting of the set of policies that follow, establishes the minimum requirements and responsibilities for the protection of Axio information assets, preventing the misuse and loss of information assets, establishing the basis for audits and self-assessments, and preserving Axio management options and legal remedies in the event of asset loss or misuse.
Applies To:	This policy applies to all Axio computer systems and facilities. This policy applies to all employees, partners, and third parties with access to Axio information assets.
Last Updated:	August 21, 2019

Key Control Listing

"KC #" references throughout the Axio ISP refer to key controls that Axio relies on to mitigate key information security risks identified by Management. These key controls have been cross-referenced to the SOC 2 criteria to ensure that Management remains in compliance with the SSAE 18 – SOC 2 requirements. The key control listing appears in Appendix A at the end of this Information Security Policy and Procedures (ISP) document.

Version Control

See Appendix B at the end of this ISP document.

Program

Information Security Program - Axio has a comprehensive, written information security program that secures Axio information assets in a manner commensurate with each asset's value as established by risk assessment and mitigation measures.

Axio Principle - Each and every employee has a role in ensuring the information security (confidentiality, integrity, and availability) of customer, proprietary, and all other data.

Policy and Procedures Requirements

Information Asset Security Policies - Policies have been implemented and enforced to ensure the information security (confidentiality, integrity, and availability) of Axio information assets and Axio customer data. The information security program contains policies and procedures that define [KC1.3]

- the risk management process
- enterprise-wide security controls
- security testing
- service provider oversight
- appropriate requirements for periodic review and updating of the information security program
- appropriate requirements for reporting to Axio management
- the safeguarding of customer information

Information Asset Security Procedures - Procedures have been implemented to enforce security policies and ensure the information security (confidentiality, integrity, and availability) of Axio information assets and customer data.

Accidental or Unauthorized Events - Policies have been implemented and enforced to protect Axio information assets against accidental or unauthorized modification, disclosure, or destruction.

Policy Sanctions

Policy Sanctions - Axio implements sanctions against employees and third parties who violate the written policies.

Policy Sanction Disciplinary Process - Assuming the action is inadvertent or accidental, first violations of information security policies or procedures must result in a warning, at a minimum. Second violations involving the same matter must be documented in the involved worker's personnel record, at a minimum. Additional violations will likely result in disciplinary action up to and including unpaid suspension or termination. Willful or intentional violations, regardless of the number of violations, may result in disciplinary action up to and including immediate dismissal, and depending on the severity, criminal prosecution may be pursued. [KC1.4]

Exceptions

Documented Policy Exception Process - All Axio employees responsible for information security must submit a written request for exceptions to conform to information security policies. The COO or his delegate must approve such exceptions.

Security Requirements of Business Associates - When working on business associate projects, Axio employees should abide by the more stringent of the business associate's security requirements or Axio's requirements. If the business associate's requirements are in conflict with those of Axio, Axio employees should bring the matter to the attention of senior managers for resolution.

Policy Distribution

Written Security Policy Documents - Axio management publishes written information security policies and makes them available to all employees and relevant external parties. The policies are published for employee viewing on Namely. [KC1.9]

Annual Review of Applicable Security Policies - All Axio employees and contractors must review and acknowledge acceptance of the information security policies that apply to them on at least an annual basis. Currently, Namely is used for reviews and acknowledgments; Namely login records are also available for use in determining employee compliance. [KC1.1]

Policy Review

Annual Review of Information Security Policy Documents - All Axio written information security policy documents are reviewed on an annual basis by a team consisting (at a minimum) of the COO and designees. [KC1.2]

Policy Review Input - The input to the management review of the Axio information security policy must include information related to

- any feedback from interested parties
- results of independent reviews of the policy
- the status of preventive and corrective actions
- results of previous management reviews
- process performance and information security policy compliance
- threat and vulnerability trends
- reported information security incidents
- recommendations provided by relevant authorities

Policy Review Output – Process Management - The output from the management review of the Axio information security policy includes

- any decisions and actions related to the improvement of the organization's approach to managing information security and its processes
- any decisions and actions related to the improvement of control objectives and controls
- any decisions and actions related to the improvement in the allocation of resources and/or responsibilities

Responsibility Assignment

Information Security Responsibilities - The Chief Operating Officer (COO), Dan Hirt) is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures. Dan Hirt is also responsible for internal operations security. The Designated Cybersecurity Executive (currently Dave White) is accountable for oversight and governance of the Axio information security program and reporting to the Board. Chief Product Officer (CPO) Dale Gonzalez is currently responsible for platform security. The COO and the COO's designee and the CPO and the CPO's designee constitute the Information Security Committee. They report issues to Dave White as needed.

Information security is a management responsibility, and decision-making for information security is not delegated. While specialists and advisors play an important role in helping to make sure that controls are designed properly, functioning properly, and adhered to consistently, it is the managers who are primarily responsible for information security. Management ensures that employees remain aware of their role in information security from hiring through termination. [KC1.7]

Axio executive managers Scott Kannry, Dave White, Dan Hirt, and Dale Gonzalez are responsible for reviewing identified actual, perceived, and potential policy violations and implementing appropriate processes and procedures for the effective risk management of those violations. Executive Management is responsible for implementing the information security policy, procedures, and controls to manage adherence to the policy effectively.

Information Security Resources - Management allocates sufficient resources and staff attention to adequately address information systems security.

Job Descriptions - Axio provides every employee with clear, written descriptions of their job responsibilities at the time of hire, and employee job descriptions are available to each of the employees,

upon request, and always during the annual employee review process [KC1.8] Management updates the job descriptions, as needed, based on operating environment changes.

Clear Assignment of Control Accountability - Axio management assigns and documents accountability for every internal control at Axio that it has designated as a "Key Control" (KC). [KC1.5] This accountability requires control owners to provide sufficient transparency in order that top management is kept informed about the effectiveness and efficiency of these same internal controls.

Information Ownership Assignment - The COO or his delegate must clearly specify in writing the assignment of Information Ownership responsibilities for those product systems, databases, master files, and other shared collections of information used to support production business activities. These Data/System Owners are responsible for authorizing all access requests and performing annual access audits. This requirement is addressed in multiple security policies. [KC1.6]

Worker Information Security Roles

Axio's Information Security Principle - Each and every employee has a role in ensuring the information security (confidentiality, integrity, and availability) of customer, proprietary, and all other data.

Three Categories of Responsibilities - To coordinate a team effort, Axio has established three categories, at least one of which applies to each worker. These categories are owner, custodian, and user. These categories define general responsibilities with respect to information security.

Owner Responsibilities - Information owners are the department managers, members of the top management team, or their delegates within Axio who bear responsibility for the acquisition, development, and maintenance of production applications that process Axio information. Production applications are computer programs that regularly provide reports in support of decision-making and other business activities. All production application system information has a designated owner. For each type of information, owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users have been granted access, and approve requests for various ways in which the information is utilized. [KC1.6]

Custodian Responsibilities - Custodians are in physical or logical possession of either Axio information or information that has been entrusted to Axio. While Information Technology department staff members clearly are custodians, local system administrators are also custodians. Whenever information is maintained only on a personal computer, the user is also a custodian. Each type of production application system information must have one or more designated custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information is not lost. Custodians are also required to implement, operate, and maintain the security measures defined by information owners. [KC1.6]

User Responsibilities - Users are responsible for familiarizing themselves with and complying with all Axio policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the custodian or the owner of the involved information.

Reporting Violations - Axio employees are obliged to report actual, perceived, or potential violations to the workstation security and use policy. The failure of employees to notify the senior managers about the potential violation may result in disciplinary action being taken.

Program Reporting

Annual Management Assessment - At least annually, Axio management assesses its information security and risk management programs including

- the status of the comprehensive information systems program
- updating of the risk assessment and analysis
- Management decisions for the level of risk mitigation and residual risk accepted
- service provider oversight activities and status
- the results of testing of key controls performed by internal (whenever applicable) or external auditors
- results of penetration testing activities (whenever applicable)
- Management's response to any identified deficiencies and recommendations for program changes
- reviews of annual incident response results (whenever applicable)

Program Review and Maintenance

Annual Program Updates - The information security program is updated and re-approved by Axio management annually or whenever there is a material change in the organization or infrastructure.

Risk Assessments - The information security program is updated, as appropriate, based on the results of the organization's annual risk assessment [KC2.1] and monthly Information Security Committee meetings. [KC2.2]

Information System Control Reviews – Independent - An independent and externally provided review of information systems security may be periodically obtained to determine both the adequacy of and compliance with controls.

Change Considerations - The appropriate level of expertise must be applied to evaluate whether changes in the organization or infrastructure should trigger a change to the information security program. Changes that must be considered that could require an update to the information security program are the effect of changes in

- technology
- the sensitivity of information
- the nature and extent of threats
- Axio business arrangements (e.g., mergers, alliances, joint ventures)
- customer information systems (e.g., new configurations, new connectivity, new software)

Security Program Compliance

Laws, Regulations and Contractual Requirements - For every Axio production information system, business line, and product offering, all relevant statutory, regulatory, and contractual requirements with customers are thoroughly researched, explicitly defined, and included in current system documentation.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy. Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

AT 101 – SOC 2: CC1.0. Common Criteria Related to Organization and Management
AT 101 – SOC 2: CC3.0. Common Criteria Related to Risk Management and Design and Implementation of Controls

Axio Risk Management Policy and Procedures

Purpose:	This policy defines the risk management requirements for the identification of the appropriate control posture for all Axio computer and communications information system assets.
Applies To:	This policy applies to all Axio computer systems and facilities, with a target audience of Axio Executive Management, Information Technology employees, and partners.
Last Updated:	August 21, 2019

Risk Management Process

Risk Assessment Methodology - Axio performs an Annual Risk Assessment based upon the model designed by a professional services firm specializing in risk management, outsourced audit, and compliance. It is an accurate and thorough assessment of the potential risks (manmade and natural) to the confidentiality, integrity, and availability of the company's critical and confidential information. [KC23.1] The initial facilitation team has extensive professional services and risk management experience and guides Axio's Management team on how to quantify the impact and probability of the risks discussed, assists in identifying the controls that mitigate the risk or act as compensating controls, and assists in documenting the results. Management discusses the overall impact and probability of each threat or vulnerability that is discussed becoming a measurable risk, concludes as to the overall risk rating, and identifies controls that help mitigate each risk. [KC2.1]

Risk Treatment - For every risk discussed and documented during the risk assessment, Management makes the determination as to how the risk is treated in the succeeding twelve months. The conclusion must fall into three primary categories:

1. Residual risk (after taking into consideration mitigating and compensating controls) is deemed to be reasonable and acceptable over the next twelve months.
2. All or a portion of the risk is transferred over the next twelve months to reduce the risk to an acceptable level. Examples include buying additional insurance or outsourcing a subprocess that isn't adequately controlled, etc.
3. Management determines the additional action to further remediate the risk over the next twelve months. Examples include hiring additional personnel and improving monitoring tools.

Axio assesses risk throughout the year during its quarterly Information Security Committee meetings. Risk is an essential consideration to all the infrastructure meetings, which focus on information system risks and capacity and resilience considerations. Axio's quarterly Information Security Committee meetings help ensure that information security objectives remain aligned with Axio's strategic business objectives. Thus, risks to both information security and key infrastructure projects are discussed on a quarterly basis with executive and key management. [KC2.2]

Material/Significant Information Security Risks - For every material/significant information systems security risk identified—whether through a formal risk assessment or not—management makes a specific decision about the degree to which Axio is self-insured and accepts the risk, seeks external insurance, or adjusts controls to reduce expected losses to an acceptable cost of conducting business.

Annual Evaluation of Information Security Operations - As part of the annual risk management process dealing with information security issues at Axio, the Management Team reviews what information security operational tasks are and what tasks are owned by specific key (information security) control owners. [KC1.5] The COO then determines, based on input from the IT management team, if any of the tasks should be added or if tasks should be outsourced in the future due to resource and/or expertise limitations. [KC2.10]

Information Systems Risk Management

Information Security Impact Analysis - Whenever critical or confidential data is to be placed in computers or whenever critical or confidential data is to be used in new or substantially different ways on computer systems, a risk assessment of the potential security-related impacts is performed. Specifically, the risks are discussed in the quarterly Information Security Committee meetings.

Third Party Disclosures

Information Sensitivity Screening and Disclosure to Third Parties - Prior to providing any non-public Axio information to an outsourcing firm, business partner, or any other non-governmental entity, IT Management and the Data Owners perform a risk assessment. [KC 4.2] This team, or their delegates, must then collectively agree that the risks associated with this disclosure do not present an undue threat to Axio business interests**.** Furthermore, Axio requests annual audit reports from third party vendors who have access to customer data [KC2.7]. In the event that a report is not available, Axio determines how to validate vendor activity with customer data.

Vulnerability and Threat Analysis

Vulnerability Advisories - On a weekly or more frequent basis, IT system administration staff review all information security vulnerability advisories issued by trusted organizations including GCP and US-CERT.gov for items affecting Axio systems.

Vulnerability Identification Software - To ensure that Axio technical staff has taken appropriate preventive measures, all systems considered part of the Axio customer infrastructure are protected by the native Google Cloud firewalls along with native alerting for available, customer-applicable, security patches whenever administrators access GCP. Further, Axio has auto-upgrade set on the Kubernetes cluster and are therefore getting security patches automatically as they are released.

The Axio IT staff runs remote management agents on end-user devices to identify security patch vulnerabilities on user endpoints. IT Administrators respond to items considered critical alerts in accordance with the Incident Response Policy. [KC2.8]

Unauthorized Access - Axio's IT personnel use IAM (Identity-Access Management) and Google Audit Logs to ensure access tracking of both humans and APIs to identify and log unauthorized production server

access attempts. [KC2.4] IT Administrators respond to items indicating unauthorized access or changes in accordance with the Incident Response Policy. In addition, Axio runs vulnerability scans on a regular basis. [KC2.8]

Security Fixes - Axio's COO and delegates monitor all security-related software updates, patches, and command scripts provided by vendors (e.g., GCP alerts as noted above), official computer emergency response teams (e.g., US-CERT), and other trusted third parties. Patches for which Axio are responsible are promptly installed, and tickets are created for critical vulnerabilities identified for which the resources are responsible. Further, Axio has auto-upgrade set on the Kubernetes cluster and is therefore getting security patches automatically as they are released. [KC2.3

GCP handles security patching of the firmware and operating application systems on which the application resides, as GCP serves as the hosting provider. GCP systems reside within the Google Cloud's Platform environment, which has multiple independent security and compliance audits annually (e.g., SOC 2, PCI). Management monitors the operating effectiveness of the key controls performed by GCP, as their infrastructure hosting provider, by obtaining the annual audit reports and analyzing the results of the independent auditor testing. [KC2.7].

Ongoing Infrastructure Monitoring - All Axio customer-servicing infrastructure systems are monitored continuously via Google Cloud Monitoring for system resource performance issues that might signal an information security issue. Google Cloud Monitoring and Stack Driver provide timely notifications, and Statuscake is used for endpoint monitoring. [KC2.5]

Annual Information Security Audit - Axio undergoes an independent, third-party Service Organization Control audit (i.e., SOC 2 – Type 2) annually that validates the design and operating effectiveness of its information security (confidentiality, integrity, and availability) controls. [KC2.6]

Service Level Agreements

Customer Contracts - Axio has contracts with their customers that communicate their commitments and the associated system requirements. Information regarding the design and operation of the system and its boundaries has been prepared and communicated to permit users to understand their role in the system and the results of system operation. Customers have been provided with information on how to report failures, incidents, concerns, and other complaints to appropriate personnel. [KC2.9]

Roles and Responsibilities

The following describes the key roles of the personnel who should support and participate in the risk management process. (See NIST SP 800-30.)

Information Security Committee - The Information Security Committee is composed of the IT administrators responsible for security and monitoring of production and development assets, as well as other key members of executive management. (Currently, Dale, Kevin, and Dan form the committee.) In addition to discussing existing risks, threats and vulnerabilities, the team identifies risks mitigated by controls already in place. Remaining residual risks are categorized as either major or minor and are included in the analysis of the effectiveness of the security protection on the environment in the scope of the specific risk.

Executive Management - Executive Management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision-making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of Executive Management.

Chief Operations Officer (COO) - The COO is responsible for the enterprise's IT planning, budgeting, and performance, including its information security components. Decisions made in these areas should be based on an effective risk management program.

System and Information Owners - The system and information owners are responsible for ensuring that proper controls are in place to address the confidentiality, integrity, and availability of the IT systems and data they own. Typically, the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

Business and Functional Managers - The managers responsible for business operations and the IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the tradeoff decisions essential to mission accomplishment. They are responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing the IT system in question for operation. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, provides mission effectiveness with a minimal expenditure of resources.

IT Security Practitioners - IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their respective IT systems. As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, and introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems. For Axio, these practitioners are often the system and/or key control owners. Professional services firms are consulted as needed.

Security/Subject Matter Professionals - The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

NIST SP 800-30 – Risk Assessment Guide
AT 101 – SOC 2: CC1.0. Common Criteria Related to Organization and Management
AT 101 – SOC 2: CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls
AT 101 – SOC 2: CC4.0 Common Criteria Related to Common Criteria Related to Monitoring of Controls
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101 - SOC 2: CC6.0 - Common Criteria Related to System Operations
AT 101 – SOC 2 – A1.1 to A1.3 – Additional Criteria for Availability
ISO/IEC 27001:2013 – 6.1.2 & 8.2 Information Security Risk Assessment
HIPAA 164.308(a)(1)(ii)(A) – Risk Analysis
HIPAA 164.308(a)(1)(ii)(B) – Risk Management
HIPAA Security Rule 164.308(a)(8) – Evaluation

Axio Personnel Security Management Policy and Procedures

Purpose:	This policy defines the information security related requirements that impact the hiring, ongoing management, and termination of personnel at Axio.
Applies To:	This policy applies to all Axio computer systems and facilities, including those managed for Axio's customers. This policy applies to all employees, partners, and third parties that perform personnel-related activities.
Last Updated:	August 21, 2019

Roles and Responsibilities

Information Security Responsibility - Responsibility for information security on a day-to-day basis is every worker's duty. Specific responsibility for information security is *not* solely vested in the IT and Engineering Departments.

Job Descriptions - Specific information security responsibilities are incorporated into the job descriptions of workers who have access to critical or confidential data. [KC1.8]

Performance Evaluations - Compliance with information security policies and procedures are considered in all employee performance evaluations. Axio's employees receive performance evaluations at least annually to ensure they remain aware of their role in ensuring the information security (confidentiality, integrity, and availability) of customer data, among their other job responsibilities. [KC3.5]. Additionally, for skilled roles requiring industry certification, an annual evaluation of training needs is performed, and CPEs are tracked as needed.

Pre-Employment Screening

Background Checks - All workers to be placed in computer-related positions of trust must pass a background check. [KC3.1] This process includes examination of criminal conviction records, lawsuit records, driver's license records, and reference checks or other verification of previous employment.

New Hire Vetting - All workers are vetted for competency, and documentation is maintained in Greenhouse. Personality and problem solving tests are given to all potential new hires. [KC3.8]

Terms and Conditions of Employment

Required Acknowledgments for System Access - Users must sign the Axio Code of Conduct and Information Security Policy acknowledgement forms prior to being issued access to Axio's systems. [KC3.2] They are also required to sign the Axio non-disclosure agreement. [KC3.3] In addition, Management completes an onboarding checklist in Script for new hires evidencing approval for system access. [KC3.7]

Property Rights - Without specific written exceptions, all programs and documentation generated by or provided by any worker for the benefit of Axio are the property of Axio. Management ensures that all workers providing such programs or documentation sign a statement to this effect prior to the delivery of these materials to Axio.

Non-Disclosure Agreements – Organization - All contractors and third-party providers to Axio with network and/or confidential data access must personally sign an Axio non-disclosure agreement before work begins. If a worker has been working without a non-disclosure agreement, a signature must be provided as a condition of continued employment. [KC3.3]

Intellectual Property Rights - As a software provider, Axio is exposed to exceptional risks, particularly the loss of intellectual property and security problems in Axio software. Therefore, appropriate measures must be taken as part of the Axio development and support processes to protect Axio's own innovations and to ensure that the security and data protection requirements in Axio software and product development are observed. While employees of Axio, all staff members grant to Axio exclusive rights to patents, copyrights, inventions, and all other intellectual property they originate or develop.

Code of Conduct Acknowledgement - All workers indicate their understanding of the code of conduct by signing the Axio Code of Conduct acknowledging that they agree to subscribe to the standards of conduct it describes. [KC3.2]

Conflicts of Interest - All workers avoid actual or apparent conflicts of interest in their business-related dealings as described in the Axio Code of Conduct and the Axio Conflict of Interest Policy. Should there be any doubt as to the existence of a potential conflict of interest, the worker should consult his or her manager.

Security Awareness and Training

Security Violations and Reporting - Users are clearly informed about the actions that constitute security violations as well as informed that all such violations will be logged and how to properly report possible security incidents.

Information Security Policy Distribution - On or before their first day of work, all new Axio workers receive a copy of the Information Security Policy and are made aware that they are required to comply with the requirements described in its set of policies as a condition of continued employment.

Policy Work Agreement - Every worker should clearly understand the Axio policies and procedures about information security and agree to perform his or her work according to those policies and procedures. [KC3.2]

Information Security Policy Changes - All Axio workers are informed of any changes in Axio's Information Security Policy, including how these changes may affect them, and how to obtain additional information.

Annual Information Security Class - All employees and partners complete an information security training course and pass a corresponding test on an annual basis. New workers are required to attend and pass the course upon hire and subsequent training. [KC5.1] Employees are required to attend continued training annually that relates to their job roles and responsibilities. [KC3.9]

Training Verification Record - To provide evidence of employee attendance, HR maintains a tracking worksheet that confirms that all employees have attended the Information Security Awareness class, understood the material presented, and had an opportunity to ask questions.

Training Records - Management maintains a listing of the training provided to all users of Axio's information assets. Axio employees provide documentation of any professional development training and events that are funded by Axio.

Personnel Self-Study - Axio employees are expected to maintain a basic understanding of cybersecurity concepts and controls as well as general situational awareness with regard to emerging cyber threats.

Social Media

Axio employees must not post critical or confidential data, insider information about business associates, or negative information about Axio to social media.

Axio employees must not use social media to communicate regarding sensitive Axio business. If questions on social media platforms emerge, Axio employees should communicate directly with senior managers.

Segregation of Duties

Separation of Duties - Whenever Axio's computer-based process involves confidential, valuable, or critical information, the system includes controls involving a separation of duties or other compensating control measures that ensure that no one individual has exclusive control over these types of information. Due to the nature of the service which Axio provides to its customers, there are some privileged user IDs needed to perform their duties that create SOD issues by default. Nonetheless, Axio has developed a detailed Access Policy and Procedures to create a monitoring mechanism which serves as a compensating control.

Personnel Transfers and Changes

Reporting Status Changes - Employees have a duty to promptly report to their immediate manager all changes in their personal status which might affect their eligibility to maintain their current position. Examples of such status changes include convictions for crimes and outside business activities.

Personnel Terminations

Temporary Worker Transfers - Workers who have given notice of their intention to leave the employment of Axio, as well as those who are aware of an impending involuntary employment termination, are transferred to positions where they can do minimal damage to Axio's assets. This policy also applies to those workers who are known to be disgruntled. At the worker's supervisor's option, these individuals may alternatively be placed on a paid leave of absence.

Immediate Terminations - Unless the special permission of a COO is obtained, all workers who have stolen Axio's property, acted with insubordination, or been convicted of a felony, are terminated immediately. Such instant terminations involve both escort of the individual off Axio's premises, as well as assistance in collecting and removing the individual's personal effects.

Worker Termination Responsibility - In the event that an employee, consultant, or contractor is terminating his or her relationship with Axio, the worker's immediate manager and HR representative ensure that the rest of the organization is notified in a timely manner. All changes to worker access for an employee or contractor are tracked through Axio's ticketing system to provide accountability and tracking on all changes in employee access privileges. The Termination Checklist is used to ensure that all property in the custody of the worker is returned before the worker leaves Axio. [KC3.6] Notification should be given to administrators handling the computer and communications accounts used by the worker as soon as the termination is known and terminate all other work-related privileges of the individual at the time that the termination takes place. The same process is followed for terminated third-party contractors and others who have been granted access to Axio systems or facilities using Slack. [KC3.4]

Notification of Worker Terminations - All employees should be immediately notified as soon as a worker has been terminated. With each such notice, the Executive Management team should regularly remind employees that departed workers are no longer permitted to be on Axio's property (unless escorted by an employee), use Axio resources, or in any other way be affiliated with Axio.

Notification to Third Parties of Worker Terminations - If a terminated worker had authority to direct contractors, consultants, or temporaries, or if this same worker had the authority to bind Axio in a purchase or another transaction, the Executive Management team promptly notifies all relevant third parties that the terminated worker is no longer employed by Axio. [KC3.4]

Involuntary Terminations - In all cases where information technology support workers are involuntarily terminated, they are immediately relieved of all of their duties, required to return all Axio's equipment and information, and escorted while they pack their belongings and walk out of Axio's facilities. [KC3.4]

Information Retention at Employment Termination - Upon termination of employment, workers may not retain, give away or remove from the Axio premises any Axio information other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other Axio information in the custody of the departing worker is provided to the worker's immediate supervisor at the time of departure.

Recovery of Organization Property - Employees, temporaries, contractors, and consultants do not receive their final paycheck unless they have returned all hardware, software, working materials, confidential information, and other property belonging to Axio. See process described above.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy should provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

HIPAA: Workforce Security 164.308(a)(3)
MA 201 17.03 (2) (b) (1) Security Program - Employee Training
ISO/IEC 27002:2013 – 7.0 Human Resources Security
AT 101 – SOC 2: CC1.0 Common Criteria Related to Organization and Management
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 – SOC 2: CC4.0 Common Criteria Related to Common Criteria Related to Monitoring of Controls
AT 101 – SOC 2: CC5.0 Common Criteria Related to Logical & Physical Access Controls
AT 101 – C1.4 and C1.6: Additional Criteria for Confidentiality

Axio Third-Party Security Management Policy and Procedures

Purpose:	This policy defines the requirements for the management of third-party services that handle critical or confidential data for Axio in any manner.
Applies To:	This policy applies to all Axio's computer systems and facilities, including those managed for Axio's customers. This policy applies to all employees, partners, and third parties with access to Axio's information assets.
Last Updated:	August 21, 2019

Third-Party Security Requirements

Third-Party Risk Assessment - When using a third party to manage information processing facilities, all risks are identified in advance, mitigating controls are established, and all contractor expectations are incorporated into the contract for these services. [KC4.1]

Third-Party Access Terms and Conditions - Before any third party is given access to Axio's systems, a contract defining the terms and conditions of such access is signed by a responsible manager at the third-party organization and approved by Axio. [KC4.1]

Third-Party Information Security Responsibilities - All of Axio's business partners, suppliers, customers, and other business associates are made aware of their information security responsibilities through specific language appearing in contracts that define their relationship with Axio.

Third-Party Access Control

Please note: The policy statements in this section are not applicable, since Axio currently does not have any internal networked computer systems.

Third-Party Access to Internal Systems - Third-party access to any Axio's internal computer systems that are not clearly public are approved in advance by the COO or a designee.

Third-Party User IDs - In the event that Axio grants a third party system access, before a user ID can be issued to a third party, documentary evidence of an information security system or process is provided to and approved by Axio's COO, and the third party agrees, in writing, to maintain this system or process to prevent unauthorized and improper use of Axio's systems. The access and permissions authorization are based on Access Control Policy and evidenced via ticket. [KC4.3]

Information Exchange

Third-Party Critical or Confidential Data Handling - All disclosures of critical or confidential Axio data to third parties are accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used. Axio requires third parties who handle critical or confidential Axio data to acknowledge Axio's Information Security, Acceptable Use, and Data Confidentiality policies and procedures. [KC4.4]

Third-Party Non-Disclosure Agreements - Axio does not currently allow any third-party access that could result in a threat to customer confidentiality. However, in the event that Axio would grant access or send any critical or confidential data to a third party for copying, printing, formatting, or other handling, the third party is required to sign Axio's non-disclosure agreement. [KC4.5]

Third-Party Information Disposal - Third-party partners and contractors are not to retain any proprietary or confidential information without the express consent of Axio and the customer.

Third-Party Contracts

Control Measures in Outsourcing Contracts - All information technology outsourcing contracts include specific words defining the control measures that are provided and maintained.

Outsourcing Contract Approvals - All outsourcing contracts related to information systems are reviewed and approved by the COO, who is responsible for ensuring that these contracts sufficiently define information security responsibilities, how to respond to a variety of potential security problems, and the right to terminate the contract for cause if it can be shown that the outsourcing organization does not abide by the information-security-related contractual terms. [KC4.1]

Annual Review - Axio conducts reviews on their critical vendors at least annually and retains documentation of these reviews. [KC4.2]

Reporting Third-Party Security Violations - All outsourcing contracts stipulate that the third parties notify Axio immediately of any security incident likely to impact critical or confidential Axio data under their control. Axio retains the right to aid in the investigation of these incidents. See Axio's Incident Management P&P for additional details.

Outsourcing Security Violations - All third-party outsourcing contracts stipulate that the contract may be terminated due to information security violations by the outsourcing partner.

Personnel Security

Non-Employee Background Checks - Temporaries, consultants, contractors, and other third-party organization staff are not given access to Axio critical or confidential data or allowed to access critical information systems unless they have gone through a background check commensurate with the background checks given to regular employees. [KC3.1]

Assessment, Monitoring and Audits

Third-Party Auditing Agreements - All agreements dealing with the handling of Axio information by third parties include a clause granting permission to Axio for the periodic auditing of the controls used for these information handling activities and specifying the ways in which Axio's information is protected. As GCP has physical and environmental control responsibility as part of their cloud services offerings utilized by Axio, Management reviews the testing performed by independent auditors, as documented in Section 4 of GCP's annual SOC 2 report, to validate the operating effectiveness of GSP's security controls to meet this control. [KC4.2]

Third-Party Notice of Business and Technical Changes - Arrangements with information systems outsourcing firms are structured such that Information Technology Department management receives notices of all material changes in the outsourcing firm's business and technical environment. Such notices should be received well in advance of such changes actually taking effect.

Contingency Plans

Continuity Service Level Agreements with Third Parties - All agreements with third parties, such as suppliers, service providers, and business partners, that could negatively impact the business processes of Axio define service level agreements and require minimum standards of contingency planning and preparation on the part of these third parties. [KC4.1]

Contract Failure Remedies - In addition, the contract language of these service level agreements specifies remedies to Axio in compensation for losses incurred by failure to put the Company's needs at the specified priority or service level. [KC4.1]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

MA 201 CMR 17.03 (1) - Security Program Requirements
HIPAA Security Rule 164.308(a)(1): Security Management Process
HIPAA Security Rule 164.308(b)(1): Business Associate Contracts and Other Arrangements
HIPAA Security Rule 164.308(b)(4): Written Contracts and Other Arrangements
AT 101 – SOC 2: CC1.0. Common Criteria Related to Organization and Management
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 – SOC 2: CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls
AT 101 – SOC 2: CC4.0 Common Criteria Related to Common Criteria Related to Monitoring of Controls
ISO/IEC 27002:2013 – 15 Supplier Relationships
ISO 27002 - 6.1.1 Management commitment to information security

Axio Data Confidentiality Policy and Procedures

Purpose:	The purpose of this policy is to detail how critical or confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of critical or confidential data and outlines specific security controls to protect this data.
Applies To:	The scope of this policy covers all company-confidential data, regardless of location. Also covered by the policy are hard copies of company data such as emails, printouts, faxes, and notes.
Last Updated:	August 21, 2019

Overview

Critical or confidential data is the data that holds the most value to the company as well as to external parties. (For brevity, "confidential" is used for "critical or confidential" throughout this section.) Most often, confidential data can carry greater risk than general company data. Lastly, confidential data represents the information retained by the company that is subject to federal and state privacy laws. For these reasons, Axio has implemented security standards that relate specifically to confidential data.

Treatment of Confidential Data

For clarity, the following sections on storage, transmission, destruction, and labeling of confidential data are restated and clarified from the Data Classification Policy and Procedures.

Access

Management embedded key controls throughout the Information Security Policy (herein) addressing the granting and authorization of access to confidential data and systems. At a minimum, confidential data access is authorized by the functional Department Manager as well as the data/system owners (as defined by the Company). [KC5.2] Privileged user access into confidential data environments requires even further scrutiny. During access reviews, reviewers challenge the necessity of users who currently have access to confidential data/systems for appropriateness. [KC5.3]

Storage

Confidential data, as defined in the Data Classification P&P, must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential data should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured. Confidential data is secured as detailed in the Security Controls for Confidential Data section below and stored in compliance with the Backup and Recovery P&P.

Axio has concluded that the most critical data within the organization is not only the customers' data but also the user passwords and, in particular, privileged user (admin, root, etc.) passwords to the various core infrastructure systems and applications that receive, process, or store the relevant data.

Therefore, Management ensures that employee and all application user passwords are encrypted at rest and not stored elsewhere. Full database encryption is used to store critical or confidential customer data, whenever possible. Okta is used for internal users, and passwords are encrypted within AWS Cognito for authentication. [KC5.4] Additionally, at the application level, Axio enforces https for authentication and other data inputs to provide encryption in transit, and passwords at rest are hashed and stored as well.

Axio employees store Axio data and confidential client and other business associate data only in the Axio instance of Box, a secure file sharing platform, unless other requirements are presented by the business associate. When sharing files with clients and other business associates on Box, an Axio best practice is to use named external collaborators and not anonymous shared links. (We get free external collaborators with the Box Enterprise Edition.)

If the use of removable media is required, Axio employees ensure that any confidential data is encrypted.

Transmission

Confidential data must not be transmitted outside the company network without the use of strong encryption. In addition, the customer infrastructure has been configured to only be accessible by Axio employees via an encrypted channel. [KC5.6]

Axio enables customer users to always access the Axio application over an encrypted channel (i.e., https); however, the user determines the pathway. [Noted in SOC 2 Report – User Entity Control]

Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following general guidelines apply:

- Paper documents: Crosscut shredding is required.
- Storage media (CDs, DVDs): Physical destruction is required.
- Hard drives/systems/mobile storage media: At a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially available methods for data wiping. Alternatively, the company has the option of physically destroying the storage media. See Information Disposal policy and procedures for additional details which incorporate NIST SP 800-88 regarding Data Sanitization. See the Information Disposal P&P for additional details.

Labeling

Physical documents containing critical or confidential data as defined within the ISP should be created only if absolutely necessary. Documents containing confidential data must be labeled either at the top or bottom of each page or through use of a watermark embedded into the background of each page if physical documents are created.

Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to the company's standards involving the treatment of confidential data. Therefore, employees are required to annually acknowledge with a signature that they understand and adhere to the Axio Data Confidentiality Policy.

The following applies to how users must interact with confidential data:

- Axio users are advised of any confidential data they have been granted access to by their manager and/or the data owner(s). As noted, all customer data as well as Axio infrastructure and application passwords are designated as confidential.
- Users must access confidential data only to perform their job function.
- Users must not seek personal benefit or assist others in seeking personal benefit from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute or disclose the information unless necessary to do their job or the action is approved by their supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to their supervisor.
- If confidential information is shared with third parties, such as contractors and vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Not under any conditions is confidential data disclosed to any third party unless that third party has been specifically authorized by Axio's COO to receive that information and has entered into a confidentiality agreement. Refer to the Third-Party Security Management P&P for additional guidance.

Security Controls for Confidential Data

Note: See referenced policies for Key Control details.

Confidential data requires additional security controls in order to ensure its integrity. The company requires that the following guidelines are followed:

- Employees should ensure that customers are aware that strong encryption is available for confidential data transmitted external to the company. For instance, if critical or confidential data is to be sent to a customer, Axio requires that data be encrypted prior to being emailed or shared via an encrypted folder sharing service. (See Email Security P&P.)
- Customer and partner reports and data containing personally identifiable information provided to Axio is shared via encrypted files and folders.
- Employees are not to store confidential data, as defined within this policy, on mobile devices or removable computer media. If it must be stored for business reasons, employees should consult their supervisor and the COO in order that an encryption application can be utilized to store the data in an encrypted form.
- Network segmentation of confidential data is utilized to limit access pathways. (See Network Security Management P&P.)
- Strong passwords must be used for access to confidential data. (See Account Management P&P and Password Management P&P.)

- Systems that contain confidential data are secured in compliance with Network Security Management P&P, Firewall Management P&P, and Access Control Policy and Procedures.
- Production databases are to be encrypted at rest, whenever possible. [KC5.5]
- When printing confidential data, the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas. Printed confidential data must contain the "Confidential Data" label. (See Physical Security P&P.*)*
- When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent, and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas. (See Physical Security P&P.*)*
- Employees must consider using an encrypted folder (e.g., Google Drive) for communicating confidential data, as defined, if it is to be emailed outside the company. (See Email Security P&P.)
- If confidential information is mailed outside the company, the user must use a service that requires a signature for receipt of that information.
- When confidential information is discussed it should be done in non-public place and where the discussion cannot be overheard.
- Confidential data must be removed from documents unless its inclusion is absolutely necessary.
- Confidential data must never be stored on non-company-provided machines (i.e., home computers). Axio recognizes that company email can oftentimes contain critical or confidential data. As noted above, employees are responsible for encrypting emails that they send containing critical or confidential data as defined herein. In addition, employees are encouraged to protect their mobile devices with which they access the corporate email system with additional access controls such as a password. Axio has the right to remove Axio content or Axio data from a personal or mobile device.
- If critical or confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.

Examples of Confidential Data

The following list is not intended to be exhaustive but should provide Axio employees with guidelines on what type of information is typically considered confidential. Confidential data has been defined and communicated during security awareness training. [KC5.1]

Confidential data includes

- customer personally identifiable information (PII), such as customer account IDs, names, addresses, locations from receipt through output
- encryption keys protecting user authentication and customer data
- employee PII, such as addresses, Social Security numbers, dates of birth
- all unique and privileged user IDs and passwords that access the Axio infrastructure
- all Axio infrastructure and access schematics

Emergency Access to Data

Confidential and critical data is accessible during an emergency through several different available methods to ensure access is always available. These include data stored on third-party SaaS tools that provide a copy stored on the user's system and copies available through a web interface.

Changes to Confidentiality Policy

If the confidential commitments, requirements, and responsibilities change for customers, third parties, or contractors, Axio will notify them via email and update their contracts.

Applicability of Other Policies

This document is an integral part of the company's cohesive set of information security policies. Other policies may apply to the topics covered in this document and should be reviewed as needed.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101 – SOC 2 – C1.1 to C1.6 – Additional Criteria for Confidentiality
HIPAA Security Rule 164.312(a)(2)(iv): Encryption and Decryption (of ePHI)
HIPAA Security Rule 164.312(e)(2)(ii): Encryption (in transmission)
ISO/IEC 27002:2013 – 9 Access Control
NIST 800-53 - Security and Privacy Controls for Federal Information Systems

Axio Data Classification Policy and Procedures

Purpose:	The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified. This policy and procedures should be read in conjunction with the Data Confidentiality Policy.
Applies To:	The scope of this policy covers all company data stored on Axio-owned, Axio-leased, Axio-approved, and otherwise company-provided systems and media, regardless of location. Also covered by the policy are hard copies of company data, such as printouts, faxes, notes, etc.
Last Updated:	August 21, 2019

Overview

Information assets are assets to the company just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to company operations and the confidentiality of its contents. Once this has been determined, the company can take steps to ensure that data is treated appropriately.

Data Classification

Data residing on corporate systems must be continually evaluated and classified into the following categories:

Personal	Includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.
Public	Includes already-released marketing material, commonly known information, etc. There are no requirements for public information.
Operational	Includes data for basic business operations, communications with vendors, employees, etc. (non-confidential). The majority of data falls into this category. Employees are to use their professional judgment in the handling and storage of operational data. Employees should seek guidance from their direct supervisor if questions arise. If an employee remains unsure or uncomfortable with how particular data is being handled and/or stored, guidance from the COO should be sought to ensure appropriate treatment.
Critical and/or Confidential	Any information deemed critical to business operations (often this data is operational as well). Examples of critical or confidential data include • any data received from customers • encryption keys protecting user and device authentication • all unique user IDs and passwords that access the Axio infrastructure • all privileged user IDs and passwords that access the Axio infrastructure

	• employee or customer personal information including addresses, Social Security numbers, dates of birth, etc. (i.e., PII) • all Axio infrastructure and access schematics See the Confidential Data Policy for more detailed information about how to handle confidential data.

At a minimum, Axio's Management Team reassess on a regular basis the classifications and locations of all data to ensure that sufficient security protections are applied to all data received, processed and stored by the Company. [KC 6.1]

Employees are to use their professional judgment in the handling and storage of critical data. Employees should seek guidance from their direct supervisor if questions arise. If an employee remains unsure or uncomfortable with how particular data is being handled and/or stored, guidance from the COO should be sought to ensure appropriate treatment.

Data Storage

The following guidelines apply to storage of the different types of company data.

Personal	There are no requirements for personal information.
Public	There are no requirements for public information.
Operational	Operational data must be stored on a server that is backed up on a daily basis (refer to the Backup Policy for additional information). System or disk-level redundancy is required.
Confidential	Critical and/or confidential data must be stored on a server that is backed up on a daily basis (refer to the Backup Policy for additional information). System or disk-level redundancy is required. Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use (clean desk, clean screen policy). Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured. Confidential data must be stored on a server that is backed up on a daily basis (refer to the Backup Policy for additional information).

Data Transmission

The following guidelines apply to transmission of the different types of company data.

Personal	There are no requirements for transmission of personal information.
Public	There are no requirements for transmission public information.
Operational	No specific requirements apply to transmission of operational data; however, as a general rule, the data should not be transmitted unless necessary for business purposes.

Confidential	*Confidential data must not be transmitted outside the company network* without the use of strong encryption. Only secure protocols are permitted for data transit between applications and servers in the production environment.

Data Destruction

The following guidelines apply to the destruction of the different types of company data.

Personal	There are no requirements for personal information.
Public	There are no requirements for public information.
Operational	There are no requirements for the destruction of Operational Data, though shredding is encouraged.
Confidential	Confidential data must be destroyed in a manner that makes recovery of the information impossible. [KC6.2] The following guidelines apply: • Paper documents: Crosscut shredding is required. • Storage media (CDs, DVDs): Physical destruction is required, preferably by an authorized vendor. The Axio Information Security Committee or COO are to be consulted whenever customer data is to be transported or destroyed. • Hard drives/systems/mobile storage media: At a minimum, data wiping is used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially available methods for data wiping. The Information Security Committee, COO, and/or the NIST 800-88 are to be consulted. When needed, the company uses onsite shredding and/or destruction of media. See the Information Disposal P&P for additional guidance.

Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document, and those applicable policies should be reviewed as needed. In particular, understanding and adherence to the Data Confidentiality Policy is a critical control objective for all employees.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

HIPAA Security Rule 164.308(a)(7)(ii)(E): Applications and Data Criticality Analysis
HIPAA Security Rule 164.312(a)(2)(iv): Encryption and Decryption (of ePHI)
HIPAA Security Rule 164.312(e)(2)(ii): Encryption (in transmission)
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 – SOC 2: CC3.0 Common Criteria Related to Risk Management & Design and Implementation of Controls
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
ISO/IEC 27002:2013 – 8.2 Information Classification

Axio Asset Management Policy and Procedures

Purpose:	This policy establishes the minimum requirements and responsibilities for the protection of Axio's information assets, preventing the misuse and loss of information assets, establishing the basis for audits, and preserving Axio management options and legal remedies in the event of asset loss or misuse.
Applies To:	This policy applies to all Axio computer systems and facilities, including those managed for Axio's customers. This policy applies to all employees, partners, and third parties with access to Axio's information assets.
Last Updated:	August 21, 2019

Asset Procurement

Hardware and Software Procurement - All hardware and software must be procured through the purchasing process according to company IT needs.

Vendors Providing Mission Critical Hardware, Software, and Services - All Axio mission critical hardware, software, and services must be purchased, rented, leased, or otherwise obtained from a trusted and well-established vendor who is able to provide maintenance services and warranties.

Asset Inventory

Asset Inventory – Technology - The IT team must prepare an annual inventory of production information systems detailing all existing production hardware, software, and communications links. GCP and AWS Dashboard serves as the primary tool for maintaining an up-to-date inventory of Axio production assets [KC7.1]

Axio IT personnel ensure that hardening baselines are met whenever a device is commissioned or changed (see Infrastructure Change Management P&P), and when new devices are deployed that they appear in or are added to the GCP monitoring tools and the patch management and antimalware monitoring tools (as required).

End-user device inventory is managed using Jamf. [KC7.1]

Asset Inventory Contents - Every asset recorded in the asset inventory includes the following information:

- asset name
- asset location
- security classification
- hardware and software configurations

Equipment Authorization

Approved Security Configuration - All computers and communications equipment used to access the Axio customer platform and all other Axio data, including personal computers, mobile devices, and smartphones, must be configured according to standards approved by the COO. Axio requires, at a minimum, that end users maintain settings that allow for automatic updates of OS security patches and antivirus/antimalware software. Employees who are unsure whether their equipment meets these criteria must contact the IT Department, who will confirm that that they are receiving the necessary updates.

Axio achieves timely end-user device maintenance by using Jamf. Approved security configurations on end-user devices are achieved by the Jamf agent automatically downloading/updating the hardened profile whenever a user connects to the internet. [KC7.2] In order to function, Jamf requires that a program be installed on each managed device (i.e., the Jamf Binary). All Axio employees are absolutely prohibited from removing or attempting to alter the Jamf Binary from a managed device. Exceptions may be granted by Axio senior managers, but only for temporary removal in a test environment as part of the Jamf setup and testing.

Axio employees apply software and security updates to devices and applications used to process Axio data. The following patching guidelines are to be followed by all Axio employees for all Axio devices:

- Check for new updates at least weekly and apply them to operating systems and software applications as soon as possible after the release of such updates.
- Apply updates and patches that are required by Axio within five working days.
- Research and apply any updates and patches required to mitigate an emergent, novel cybersecurity threat within 5 working days unless otherwise advised by Axio.

Property Removal

Decommission of Mobile Devices - All Axio-issued mobile devices, including laptops, PDAs, and cell phones, must be returned to Axio when no longer in use by employees or contractors.

Property Reuse and Disposal

Approval for Third-Party Removal of Any Equipment - Before Axio equipment of any type is sold, disposed of, recycled, donated, or otherwise conveyed to a third party, the COO or his delegate must give approval and the Asset Disposal P&P must be followed.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – 8.1 Responsibility for Assets
HIPAA: Device and Media - Accountability (A)
AT 101 – SOC 2: CC4.0 (Monitoring), CC5.0 (Access) and CC6.0 (System Operations)
AT 101 – SOC 2: CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls

Axio Information Disposal Policy and Procedures

Purpose:	This policy defines controls for the proper disposal of all Axio critical or confidential data either in paper or electronic format.
Applies To:	This policy applies to all Axio computer systems and facilities, including those managed for Axio customers. This policy applies to all employees, partners, and third parties with access to Axio information assets in digital or hardcopy form.
Last Updated:	August 21, 2019

Information Disposal Standards

Data Sanitization Standards - The COO is responsible for establishing standards for the proper sanitization of all computer equipment and media storage scheduled for destruction. These same standards are used by the third-party vendors contracted to dispose of Axio's equipment. Laptops are wiped remotely using Jamf; all customer data is wiped, and completion is communicated to the customer. [KC8.1]

Axio's physical infrastructure where customer data resides is hosted and managed within Google's secure data centers and uses the Google Cloud Platform (GCP) technology. GCP uses techniques outlined in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data.

Roles and Responsibilities

Information Security - The COO is responsible for establishing standards for the proper identification and labeling of Axio information according to sensitivity levels. See the Data Classification Policy and Procedures for additional details. The department is also responsible for establishing detailed standards for the proper destruction of electronic data to implement this policy.

Data Owners - Axio is the primary confidential data owner. Nevertheless, for systems owned and controlled by Axio that house customers' confidential data, Axio has assigned data owners who are responsible for ensuring that all Axio data under their ownership is properly destroyed according to this policy. See the Data Confidentiality P&P for additional details.

Users - All users of computer systems within Axio, including contractors and vendors with access to company systems, are responsible for taking the appropriate steps outlined below to ensure that all computers and electronic media are properly sanitized before disposal.

Record Retention

Customer Data - Axio does not keep customer personal data for a longer period than is necessary in relation to the purpose for which the data was collected. Customer data is retained as long as Axio is contractually obligated to process the data.

Employee Data - Retained for seven years after employment termination or as long as legally required.

Backups - The retention of backups is detailed in the Backup and Recovery Policy.

Disposal of Hardcopy Records

Hardcopy Disposal - When disposed of, critical or confidential data in hardcopy form must be shredded using crosscut shredders.

Disposal of Electronic Media

Storage Media Destruction - Destruction of critical or confidential data captured on computer storage media must be performed only with approved destruction methods based on the policy approved by the COO.

Disposal of Electronic Media Outside of Axio - All electronic media other than computer hard drives must be erased or rendered unusable before being decommissioned. Employees must use only approved commercial vendors from the Disposal Approved Vendor List and obtain a certification confirming that the data drive was destroyed. When necessary, laptops can be wiped remotely using Jamf. When a customer decommissions, all customer data is wiped, and completion is communicated to the customer. [KC8.1]

Disposal of Computer Equipment

Used Component Equipment Release - Before disposal, donation, or recycling, the COO or his/her designee must validate that critical or confidential data has been removed from any information systems equipment that has been used for Axio business. This validation process must take place before releasing such equipment to a third party.

Transfer of Hard Drives and Media

Chain of Custody - All movement of customer and other confidential data requires approval from the Information Security Committee or the COO. Axio uses a chain of custody form whenever data in physical or electronic form is being transported to an external party (e.g., a data destruction company).

Transfer of Hard Drives - Before a hard drive is transferred from the custody of its current owner, appropriate care is taken to ensure that no unauthorized person can access the data by ordinary means. All electronic media are sanitized according to Axio procedures.

Transfer of Electronic Media - Before electronic media is transferred from the custody of the current owner, appropriate care is taken to ensure that no unauthorized person can access the data by ordinary means. Electronic media such as rewritable media are to be erased if the media type allows it (in accordance with NIST SP 800-88) or destroyed if erasure is not possible.

Attempted Recovery - Attempts to recover deleted or sanitized data is done only by specially trained personnel approved by Axio management. Insofar as special recovery tools are used by an individual to access the data erased by this method, any unauthorized attempt by an individual to access data is viewed as a conscious violation of state or federal regulations and is subject to disciplinary action up to

and including termination and prosecution. AWS maintains storage volumes from deprovisioned applications and the associated databases for one week, after which time they are automatically destroyed, rendering the data unrecoverable.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

HIPAA: Device and Media - Disposal (R)
MA 201 17.03 (2) (c) Security Program - Information Exchange
ISO/IEC 27002:2013 – 8.3.2 Disposal of Media
PCI v3.1 Requirement 9.8 – Media Destruction Policies & Procedures
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101 – SOC 2: C1.3 and C1.5 Additional Criteria for Confidentiality

Axio Physical Security Policy and Procedures

Purpose:	This policy defines the requirements for establishing physical access controls at Axio locations.
Applies To:	This policy applies to all Axio facilities and data centers, with a target audience of all employees and partners.
Last Updated:	August 21, 2019

Access Controls

Physical Access Control to Critical or Confidential Data - Access to every computer room (data center) and work area containing critical or confidential data is physically restricted to limit access to those with a need to know.

Axio locations require a badge to gain access upon building entrance. [KC9.1] All visitors must stop at the reception area and registration is required. [KC9.2].

Access to Computers and Communications Systems - Buildings that house Axio computers or communications systems are protected with physical security measures that prevent unauthorized persons from gaining access.

Unauthorized Physical Access Attempts - Workers must not attempt to enter restricted areas in Axio buildings for which they have not received access authorization.

Access Control System Records - Axio maintains records of the persons currently and previously inside Axio buildings and securely retains this information for at least three months. Axio does not have data center access. Currently, Axio employees working in offices are only tenants of buildings owned and managed by others, so this control does not apply.

Terminated Worker Access to Restricted Areas - When a worker terminates his or her working relationship with Axio, all access rights to Axio facilities are immediately revoked. [KC9.3] See the Personnel Information Security P&P for additional details.

Security Clearance Process - For an employee to obtain physical access to Axio facilities, the individual must first pass the background screening process as outlined in the Personnel Security Management P&P. Contractors should be greeted and escorted by personnel as deemed necessary while on premises. Currently, no Axio employees have been authorized to physically access the data centers. If data center access becomes possible (e.g., co-location facility), Axio will first open a ticket to add the person to the "Authorized" list.

Access Control Monitoring

Physical Access Monitoring - Method - Upon entering the building all visitors are greeted by Axio staff, who monitor the entrance and require registration during business hours. The individual offices of Axio remain locked after business hours.

Physical and Environmental Control Monitoring – Data Centers - All customer data is stored and hosted on AWS and GCP cloud services, which uses ISO 27001 and FISMA certified data centers managed by Amazon and Google, respectively. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff using video surveillance, state of the art intrusion detection systems, and other electronic means. Currently, no Axio employees have requested or have been granted physical access to the AWS data centers housing Axio applications.

To monitor the operating effectiveness of the controls of the data center providers, Axio obtains and analyzes the annual independent audit reports of third-party infrastructure support providers for exceptions. Management reviews the testing performed by independent auditors, as documented in Section 4 of AWS and GCP's annual SOC 2 report, to validate the operating effectiveness of AWS's and GCP's physical security controls. [KC9.4]

Visitors

Visitor Identification - No visitors are allowed to enter Axio facilities without being escorted by Axio personnel. No customer vendors may enter without being escorted. [KC9.2]

Access Review

Data Center Staff Access - Axio employees do not have access to the data centers where the equipment containing customer production information is housed. No in-scope systems or data reside at the corporate facility; therefore, Management relies on the annual SOC 2 audits of the AWS and GPS data centers to validate the adequacy of the physical and environmental controls maintenance. The COO (or his designee) periodically reviews the authentication mechanism at the office(s) to validate that only active employees have badges. [KC9.7]

Physical-Environmental Control Maintenance

Physical-Environmental Equipment Changes - The owners of the buildings which house the Axio offices handle the repairs and maintenance to the office space. The building is responsible for maintaining HVAC and fire suppression. [KC9.5]

As noted below, no Axio employees have access to the data centers where the equipment containing customer production information is housed. No in-scope systems or data reside at the corporate facility; therefore, Management relies on the annual SOC 2 audits of the AWS and GPS data centers to validate the adequacy of the physical and environmental controls maintenance.

Mission critical equipment is sited in areas that are secured, experience low traffic, have environmental controls, and specify guidelines for the absence of eating, drinking, and smoking. Mission critical equipment is protected from power failures and other disruptions caused by the failure in supporting

utilities. Equipment is correctly maintained to ensure its continued integrity and availability during the normal course of business and in unique circumstances as they arise.

Media Handling

Physically Accessing Equipment Containing Customer Data – No Axio employees have access to the data centers where the equipment containing customer production information is housed.

Mobile Devices

Laptops, wireless handheld devices, and any other device containing Axio data must be physically protected by the user from loss, theft, and tampering. Any loss, theft, or tampering of these devices must be immediately reported to the Information Technology Department.

Employees should take care to never leave mobile devices containing Axio data in public places, including unattended vehicles. Employees must remain aware that malware, including key loggers and reverse-shell payloads, can be downloaded via their USB drives within seconds if left unattended.

When traveling, Axio employees must maintain physical control of devices and data. It is acceptable to have another Axio employee maintain physical control of devices or data; however, Axio employees must not leave these items in the custody of strangers. When using taxi or other transport services, portable devices, including laptops, should not be placed in the trunk. Axio employees may leave devices or data in a hotel only if they are secured in a safe or a locked suitcase.

It is the responsibility of the employee to protect the physical security of mobile devices. [KC9.6]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – 6.2 Mobile Devices & Teleworking
ISO/IEC 27002:2013 - 11.1 Secure Areas
ISO/IEC 27002:2013 – 15.2 Supplier Service Delivery Management
ISO/IEC 27002:2013 – 18.2 Information Security Reviews
AT 101 – SOC 2: CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls

AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101 SOC 2 – Additional Criteria for Availability - A1.2
HIPAA Security Rule 164.310(a)(1) – Facility Access Control
HIPAA Security Rule 164.310(a)(2)(ii) – Facility Security Plan
HIPAA Security Rule 164.310(a)(2)(iii) – Access Control & Validation Procedures
HIPAA Security Rule 164.310(a)(2)(iv) – Maintenance Records
PCI v3.1 – Requirement 9: Restrict physical access to cardholder data passwords and other security parameters

Axio Account Management Policy and Procedures

Purpose:	This policy defines the control requirements for the secure management of accounts on Axio's computer and communications systems.
Applies To:	This policy applies to all Axio computer systems and facilities, with a target audience of Axio's Information Technology employees and partners.
Last Updated:	August 21, 2019

Authorization

User ID and Privilege Approval - Axio applies the principle of least privilege to users granted access to Axio infrastructure. [KC10.1] Whenever user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users, they are approved in advance by the user's immediate supervisor and the system owner/administrator. As needed, approvals may be escalated to the COO. Certain access and privileges must be authorized by the COO or his designee (see the Data Confidentiality P&P).

Access Control Authorization Requests - Requests for the addition, deletion, and modification of all user IDs, credentials, and other identifier objects on Axio's computer and communications systems are submitted on a form and requested through the Axio ticketing system and/or email from the user's immediate supervisor. The COO or his designee approves whenever confidential data and/or systems are involved as defined in the Data Confidentiality P&P (e.g., access to critical or confidential customer data fields). [KC10.1]

Granting Access to Organization Information - Access to Axio organization information such as payroll and job performance data is always authorized by a designated owner of such information and is limited on a need-to-know basis to a reasonably restricted number of people.

Granting System Privileges - Computer and communications system privileges are granted only by a clear chain of authority delegation. [KC10.1]

System Access Request Authorization - All requests for additional privileges on Axio's multi-user systems are submitted by the user's immediate supervisor and are escalated to the COO. [KC10.1]

Positive Identification for System Usage - All users are positively identified prior to being able to use any multi-user computer or communications system resources.

Critical or Confidential Data Access - Access to Axio's critical or confidential data is provided only after express management authorization has been obtained.

Awareness and Training

Documentary Evidence of User Agreement to Abide by Security Requirements - Before they are granted access to Axio's information systems, all users provide documented evidence of their agreement to comply with Axio's information security requirements. [KC1.1]

Account Definition

Non-Anonymous or Shared User IDs - All user IDs on Axio's systems are constructed according to the Axio's user ID construction standard and clearly indicate the responsible individual's name. Under no circumstances are such user IDs permitted to be generic, descriptive of an organizational title or role, descriptive of a project, or anonymous. [KC11.1]

Password sharing or the use of shared IDs is strictly prohibited. Any violations to the use of non-unique IDs must be well documented and approved by the COO. Additional security precautions (e.g., mandatory, out-of-band, MFA) should be taken in the event that a system or shared ID must be used by individual users. Use of these accounts should be monitored for appropriateness.

Reuse of User IDs - Each Axio computer and communications system user ID is unique and connected solely with the user to whom it was assigned and is not reassigned after a worker or customer terminates their relationship with Axio.

System Administrator User IDs - Where possible, system and database administrators have at least two user IDs, one that provides privileged access and is logged, and another that provides the privileges of a normal user for day-to-day work. Axio restricts administrator and other privileged-user IDs to limited, authorized users.

Axio has restricted super user access to limited individuals who provide administrative, system-level functions to Axio's infrastructure. Complex passwords that only they know are required to be able to access the privileged IDs. [KC10.2]

Guest User Accounts - Axio employees disable guest user accounts on their Axio-issued laptops.

Maintenance and Emergency Changes

Emergency Removal - Whenever emergency removal of individual user accounts and/or access privileges is necessary (e.g., cyber event, malicious behavior), Axio Executive Management must be notified and take appropriate action.

User Status Changes - Every supervisor notifies the IT department about changes in employee status within Axio (including terminations and role and job responsibility changes). IT deactivates an employee's individual user accounts and access privileges within 48 hours when that person's employment at Axio terminates. IT reevaluates individual user accounts and access privileges within 2 weeks when an employee moves to a new department or assumes a new role.

Annual Review - Axio administrators review and revalidate user privileges annually.

Access and Privilege Assignment

Read Access to Critical or Confidential Data - Workers who have been authorized to view information classified at a certain sensitivity level are permitted to access only the information at this level and at less sensitive levels.

Role-Based Access Control Privileges - The information systems access privileges of all users are defined based on their officially assigned roles within Axio. Axio uses the AWS and Google Cloud identity management tools, access control lists, and security groups to restrict access to each AWS and GCP system or service based on the user's role relative to that system or service.

Privilege Restriction – Need to Know - The computer and communications system privileges of all users, systems, and programs are restricted based on the need to know.

Application User ID Restriction - Every Axio's application user ID is restricted to use only by the application for which it was established.

Special System Privileges - Special system privileges, such as the ability to examine the files of other users, are restricted to those directly responsible for system management and/or systems security. [KC10.2]

Number of Privileged User IDs - The number of privileged user IDs are strictly limited to those individuals who absolutely must have such privileges for authorized business purposes. [KC10.2]

Operating System Command Access - End users are not permitted to invoke operating system level commands. This is achieved by restricting end users to menus that display only those activities which they have been expressly authorized to perform.

Business Production Information Updates - System privileges are defined so that non-production staff such as internal auditors, system administrators, programmers, and computer operators are not permitted to update production business information.

Default User Privileges - Administrators do not grant any privileges beyond electronic mail and word processing to any user without specific written approval from management. [KC10.1]

Customer Information Access - All identifying information about customers such as credit card numbers, credit references, and Social Security numbers are accessible only to those Axio personnel who need such access in order to perform their jobs.

Critical or Confidential Data Access - Access to critical or confidential data is granted only to specific individuals, not groups of individuals. See the Data Confidentiality Policy for additional details.

Developer Access to Production Business Information - Where access to production business information is required so that new or modified business application systems may be developed or tested, only "read" and "copy" access is granted on production machines. This access is permitted only for the duration of the testing and related development efforts and is promptly revoked upon the successful completion of these efforts.

Database Access – Direct - All direct access to any Axio database is restricted to the database administrators. All administrator IDs require complex passwords (see the Password Policy for additional details) and multifactor authentication, whenever possible. [KC10.3]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy should provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 - 9.2.1 User registration & de-registration
ISO/IEC 27002:2013 - 9.2.2 User access provisioning
HIPAA Security Rule - 164.308(a)(3)(i) Workforce Security
HIPAA Security Rule - 164.308(a)(4)(i) Information Access Management
HIPAA Security Rule - 164.312(b) Audit Controls
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 SOC 2 – CC5.1, CC5.2, CC5.3, & CC5.4 (Common Criteria Related to Logical and Physical Access Controls)
AT 101 – SOC 2 – C1.1 to C1.6 – Additional Criteria for Confidentiality

Axio Access Control Policy and Procedures

Purpose:	This policy defines the control requirements surrounding the management of access to information on Axio's computer and communications systems.
Applies To:	This policy applies to all Axio computer systems and facilities, with a target audience of Axio's Information Technology employees and partners.
Last Updated:	August 21, 2019

Access Control System

Access Control System – User ID Creation Date - Access control systems are configured to capture and maintain the creation dates for every user ID. Unique user IDs are created and used for each employee, contractor (whenever applicable), and customer. [KC11.1]

Axio grants a limited number of authorized employees database access. All infrastructure-based access is AWS and GCP IAM-controlled, and any non-programmatic access to the data is locked down and controlled via IAM users, roles, and entitlements. Application authentication of Axio user IDs and passwords occurs through AWS Cognito. [KC11.2]

Access Control System – Last Logon Date - Access control systems are configured to capture and maintain the date and time of the last logon for every user ID. [KC11.6]

Access Control System – Last Logoff Date - Access control systems are configured to capture and maintain the date and time of the last logoff for every user ID. [KC11.6]

Access Control System – Password Change Date - Access control systems are configured to capture and maintain the date and time of the last password change for every user ID.

Special Privileged Users - All multiuser computer and network systems support a special type of user ID that has broadly defined system privileges that enable authorized individuals to change the security state of systems. Privileged user IDs require complex passwords and are restricted to only a limited number of authorized personnel (see Password P&P).

Access Control System Modification - The functionality of all access control systems is not altered, overridden, or bypassed via the introduction of additional code or instructions.

Password Retrieval - Computer and communications systems are designed, tested, and controlled so as to prevent the retrieval and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form. A link is generated for all employees who require a password reset. Customers have self-service for their password resets. [KC11.4]

System Capabilities and Commands - End users are presented with only the system capabilities and commands that they have privileges to perform. Axio adheres to the least privilege standard in roles and granting permissions. Management encourages users to configure workstations and laptops to lock user

sessions after 15 minutes of inactivity. Users are then re-authenticated to gain access to their workstations. [KC11.8]

Unique User ID and Password Required - Every user has a single unique user ID and a personal secret password for access to Axio's computer systems. As noted in the Password Management P&P, complex passwords are required in order to be admitted to any Axio's infrastructure systems.

Authorization

Critical or Confidential Data Access - Access to Axio's critical or confidential data is provided only after express management authorization has been obtained. (See the Confidential Data P&P for additional details.)

Requests for the addition, deletion, and modification of all user IDs, credentials, and other identifier objects on Axio's computer and communications systems are approved by the user's immediate supervisor. If need be, it may be escalated to the COO and should be documented. [KC11.5]

Granting Access to Organization Information - Access to Axio information such as payroll and job performance data is always authorized by a designated owner of such information and is limited on a need-to-know basis to a reasonably restricted number of people. (See Confidential Data P&P).

Information System Privilege Usage - Every information system privilege that has not been specifically permitted by Axio management is not employed for any Axio business purpose until approved in writing.

Granting System Privileges - Computer and communications system privileges are granted only by a clear chain of authority delegation. All user access privileges and changes are authorized by the user's supervisor and/or the data or system owner. Authorization privileges are role based. [KC11.5]

User ID and Privilege Approval - Whenever user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users, they are approved in advance by the user's immediate supervisor and Axio's management. [KC11.5]

Owner Approval for Privileges - Prior to being granted to users, business application system privileges are approved by the applicable information owner [KC11.5].

Re-Authentication Requirement - If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to reactivate the terminal or session. [KC11.8]

Computer Access Training - Before they are granted access to any of Axio's computer systems, all Axio users complete an approved information security awareness training class that includes acceptable use and confidential data discussions.

Access and Privilege Assignment

Production Programs and Information Access - Access controls to production programs and information are configured such that production programs and information systems software support personnel are not granted access privileges except for problem resolution.

Privilege Restriction – Need to Know - The computer and communications system privileges of all users, systems, and programs are restricted based on the need to know.

User IDs Employed in Abusive Activity - All access privileges for a user ID shown to be engaged in abusive or criminal activity are immediately revoked and disciplinary actions are taken.

Personal Information Access - All identifying information about customers such as credit card numbers, credit references, and Social Security numbers, are accessible only to those Axio personnel who need such access in order to perform their jobs.

Separation of Activities and Data - Management defines user privileges such that ordinary users cannot gain access to, or otherwise interfere with, either the individual activities of, or the private data of other users.

Read Access to Critical or Confidential Data - Users who have been authorized to view information classified at a certain sensitivity level are permitted to access only the information at this level and at less sensitive levels. Administrators are encouraged to use read-only restrictions whenever possible.

Role-Based Access Control Privileges - The information systems access privileges of all users are based on their officially assigned roles within Axio.

Identify Verification - An internal password reset feature is available on the login screen. In the event the user forgets their password, a password reset link is sent to the email address on file. Upon confirming identity, the user can then reset their password. [KC11.4]

System Privileges

Number and Use of Privileged User IDs - The number of privileged user IDs are strictly limited to those individuals who absolutely require such privileges for authorized business purposes. Use of privileged IDs to access customer infrastructure is documented and approved. [KC11.3]

Limiting Special System Privileges - Special system privileges are restricted to those directly responsible for system management or security. [KC11.3]

Operating System Command Access - End users are not authorized to invoke operating system level commands.

Business Production Information Updates - System privileges are defined so that non-production staff (internal auditors, information security administrators, programmers, computer operators, etc.) are not permitted to update production business information.

Number of Privileged Groups - The number of privileged groups are strictly limited to those who absolutely must have such privileges for authorized business purposes.

Axio Laptops - Axio employees have local administrative privileges but use those privileges only when absolutely necessary for maintaining the device.

Workstation/Laptop Access

Screen Locking - Axio employees should configure their workstation screensavers to automatically lock screens after 10 minutes of inactivity and require the password to unlock the workstation or otherwise lock their screens. (If an Axio employee is using their workstation to deliver a presentation they may temporarily adjust this time or disable the automatic lockout; however, they must re-enable previous settings after the presentation is complete.) Workstations must always be locked when left unattended at any time and for any period of time.

Records

Access Control Privilege Log Retention - Computerized log records reflecting the access privileges of each user with access to the production environment servers and network are securely maintained for a reasonable period of time. [KC11.6]

Production Application System Log Contents - All computer systems running Axio's production application systems include logs that record additions and changes to the privileges of users.

Access Review

Review of Accounts Used in Applications and Middleware - Axio performs a semi-annual review of the privileges of special accounts, terminated users, etc. used for production applications or middleware.

Reauthorization of User Access Privileges - The system privileges granted to every user is reevaluated by the user's immediate manager and/or system/data owner on a semi-annual basis to determine whether currently enabled system privileges are needed to perform the user's current job duties. [KC11.7]

In addition, Management reviews the testing performed by independent auditors, as documented in the GCP and AWS annual SOC2 reports, to validate the operating effectiveness of their access management controls.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy should provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – 9 Access Control

PCI DSS 7, 8 & 9 – Restrict Access to CDE based on Need to Know; Identify and Authenticate Access & Restrict Physical Access to CDE
HIPAA Security Rule - 164.312(a)(2)(iii) Automatic Logoff
HIPAA Security Rule - 164.310(c) Workstation Security
HIPAA Security Rule - 164.312(a)(2)(i) Unique Users
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101 - SOC 2: CC6.0 - Common Criteria Related to System Operations

Related Documents

Account Management P&P
Password Management P&P
Network Security Management P&P
Remote Access Management P&P

Axio Password Management Policy and Procedures

Purpose:	The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy helps users understand why strong passwords are a necessity and helps them create passwords that are both secure and usable. Lastly, this policy educates users on the secure use of passwords.
Applies To:	This policy applies to any person who is provided an account on the organization's network or systems, including employees, guests, contractors, partners, and vendors.
Last Updated:	August 21, 2019

Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

Construction

The best security against a password incident is simple: follow a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction. Complex passwords are used to connect to both GCP and AWS. [KC12.1]

- Passwords are at least 12 characters long.
- Passwords are composed of a mix of letters, numbers, and special characters (punctuation marks and symbols).
- Passwords are composed of a mix of uppercase and lowercase characters.
- Passwords should not be composed of an obvious keyboard sequence (e.g., qwerty).
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, or your children, birthdays, addresses, phone numbers, and locations.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters: a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well; for example, an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence and then use the first letter of each word as a password. The sentence "The quick brown fox jumps over the lazy dog!" easily becomes the password "Tqbfjotld!". Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique helps make strong passwords easier for users to remember.

Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone.
- Users must not share their passwords with others (co-workers, supervisors, family, etc.).
- Users must not write down their passwords and leave them unsecured.
- Users must not check the "save password" box when authenticating to applications.
- Users must not use the same password for different systems and/or accounts.
- Users must not use the same password for personal use that they use for Axio accounts, services, and devices.
- Users must not send passwords via email
- Users must not reuse passwords.
- All default passwords for accounts or assets must be changed prior to use of those accounts or assets.

User passwords are encrypted in their respective databases and in transport. AWS and application passwords are obfuscated (encrypted or hashed) at rest. [KC12.2]

Account Lockout

Axio requires that users be locked out for a period of time after six failed access attempts on all production systems whenever possible and six times on AWS. [KC12.3] This control mitigates the risk of brute force attempts on administrator IDs or other compromised user IDs. Limitations to this control may exist in the production environment where intra-system authentication is necessary because a communication delay could result in a production application crashing. The application does not require account lockout currently.

Password Encryption

Axio requires that user passwords be kept strictly confidential. Axio requires that system passwords be encrypted at rest at the application and database level, and Axio VPN is used when on an untrusted wireless network. [KC12.4] If the Axio VPN doesn't work, Axio personnel should tether to their mobile devices or use some other secure means of encryption.

Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her password to his or her immediate manager. When a password is suspected to have been compromised, the COO must request that the user change all his or her passwords. (See the Incident Response Policy for additional details.)

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
ISO/IEC 27002:2013 – 9Access Control

Axio Network Security Management Policy and Procedures

Purpose:	This policy defines the requirements for establishing the network controls related to Axio's computer and communications systems infrastructure.
Applies To:	This policy applies to all Axio computer systems and facilities, with a target audience of Axio's Information Technology employees and partners. Axio's connection directly to production is established through a firewall maintained by Google Cloud Platform (GCP). The Remote Access Management Policy details the primary procedures and controls implemented to protect the production environment. Note: Axio does not currently maintain a corporate network in the traditional sense. The network and hosts mentioned throughout this policy and the Firewall Management Policy refer to the customer-servicing infrastructure in GCP.
Last Updated:	August 21, 2019

Please note: All references of "internal network" in this policy are to our instance of the GCP and the AWS for the platform. Axio currently does not have any internal networks or networked computer systems.

Authorization

Security Configuration - Configurations and setup parameters on all hosts attached to the Axio network comply with GCP secure configuration guidelines for each system type. Specifically, Axio production servers are hardened via access control lists and port and services restrictions. [KC13.1]

Shared Directory Systems - The use of shared directory systems (e.g., Box) that are internet connected or directly reachable through the internet are approved by the COO.

Intranet Connection Security Criteria - Axio does not maintain a traditional intranet. Email and folder sharing are maintained via the internet-based solution (Box). The COO requires that users maintain an acceptable firewall on their devices, and user privilege control is managed via an established change control process as outlined in the Account Management and Access Control P&Ps.

Internet Access Privileges - Employees acknowledge and adhere to Axio's Acceptable Use P&P, which addresses internet usage on corporate systems.

Configuration

In addition to native firewalls controlled by GCP to protect the overall GCP infrastructure, native firewall rules within GCP are used by Axio to restrict access to systems from external networks and between systems internally. Further, Axio hosts the customer infrastructure inside a Virtual Private Cloud (VPC) in GCP and the customer infrastructure systems within a VPC a private subnet. By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a security group based on the system's function. Firewall rules set by Axio within GCP restrict

access to only the inbound and outbound IPs and the ports and protocols required for a system's specific function to mitigate risk**.** Each device in the Axio production environment has been hardened to the least connectivity required for the applications to run. [KC13.1]

Public Internet Servers - Axio has very few public-IP facing devices. Axio is in the process of defining tools and processes to be used to identify potential intrusions on public-facing equipment. (The closest thing Axio has to a public-facing device is the Axio website. Axio's production systems are not public-facing.)

Communication Line Changes - Workers and vendors do not make arrangements for or actually complete the installation of voice or data lines with any carrier if they have not obtained approval from the COO.

Direct Internet Connections - Production information systems are not directly connected to the internet but instead connect through a GCP firewall and the Security Group and VPC restrictions noted above.

Systems Interfacing External Networks - As noted in the GCP SOC 2 audit report, GCP deploys new systems with the latest updates, security fixes, and GCP secure configurations, and existing systems are decommissioned as GCP's customers are migrated to the new instances. This process allows GCP to keep the environment up-to-date without affecting Axio's applications, which run in isolated environments.

In order to validate the security of the production network's configuration, Axio is in the process of defining its tools and processes for assessing network and production instance vulnerabilities. [KC13.2]

Encryption of Login Info on Transmission - Axio uses transport encryption of user authentication credentials for both its internal Office 365 and remote GCP production environment access. [KC13.6]

Network Security Zones - All of Axio's production data networks are divided into security zones. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. When Axio creates a GCP firewall rule, they specify a VPC network and a set of components that define what the rule will do. The components enable Axio to target certain types of traffic based on the traffic's protocol, ports, sources, and destinations. Axio restricts access to its environment and connectivity within its infrastructure via the VPC and firewall rules settings. Firewall rules and VPC settings are reviewed at least annually. [KC13.3]

Connections

Trusted Host Relationships - Axio's COO establishes any trusted host relationships to/from or within the customer-servicing infrastructure.

Customer data is stored in access-controlled databases. Each database requires a unique username and password that is only valid for that specific database based on the combination of customer ID with matching unique user ID and password associated with that customer ID. Customers with multiple applications and databases are assigned separate databases and accounts per application to mitigate the risk of unauthorized access between applications when contractually defined.

When deploying applications, we encourage customers to take advantage of encrypted database connections.

Network Connections with Outside Organizations - The establishment of a direct connection between Axio's systems and computers at external organizations through the internet or any other public network are approved by the COO. Currently, no such connections are permitted.

Connecting Third-Party Networks - Customers control connections used into the Axio application; therefore, they control whether data encryption is used during data transmissions. (See the Overview of Axio360 Technology and Security Architecture.)

New Network Connection Process - All new network connections; that is, changes to Security Groups, are approved and tested prior to production implementation.

Monitoring

Capacity - Axio uses Google Cloud Monitoring to monitor the firewall, application, and database servers and infrastructure routers and switches. Packets per second and CPU load are monitored in the production environment, along with the servers' memory usage, RAM, and disk space. [KC13.7]

Outdated Software - Axio runs Synk and NPM audit during frequent deploys to monitor for application-related patches. Axio relies on GCP alerts on the availability of new software when users log in to identify security patches for which Axio is responsible on its production instances. Patches are made within 30 days.[KC 13.2]

Vulnerabilities - Axio assesses vulnerabilities in its configuration and production infrastructure by periodically running the GCP vulnerability scanner, which looks for out-of-date applications and networking vulnerabilities. This serves as the intrusion detection system, which actively protects the production network in GCP. [KC13.8]

Diagrams

Network Diagram - A network diagram that illustrates all connections to components that process or store critical or confidential data, including any wireless networks, is developed and maintained. [KC13.4] (Axio's instantiation of this requirement is the Overview of Axio360 Technology and Security Architecture.)

Network Diagram Consistency - The current network diagram is consistent with Axio's firewall configuration. [KC13.4]

Internal Network Addresses - Not applicable.

Access Control

Internal Network Device Passwords – Not applicable.

Network-Connected Computers Access Control - All Axio computers that connect to the production environment are protected by a privilege access control system approved by the COO, as well as local firewalls and antivirus.

Quarterly Access Reviews - The computer and communications system privileges of all customer infrastructure systems (e.g., network, servers, routers) and applications (e.g., databases and web

applications) are audited annually to validate that terminated contractor and employee IDs have been disabled, or ideally removed, and user privileges are commensurate with job responsibilities. See the Access Control P&P for further details.

Wireless Access Points

Wireless Access Points Disabled Unless Approved - Axio has only one physical office in Georgia for its DevOps team with a single approved wireless access point. All wireless access points must be pre-approved by the CTO. There are no wireless network access points within the GCP environment.

Logical Isolation of Wireless Access Points - Axio uses WPA2 within a private subnet for its corporate users; guest users are allowed permission on a separate subnet. Further, the administrator password has been changed by Axio from the manufacturer/ISP default. [KC13.5]

Authorization and Registration of Wireless Network Devices - To gain access to the Axio production network, all wireless access points, handheld wireless computers, and all other wireless devices are authorized by an Axio representative. [KC13.5]

Wireless Configuration

Vendor Defaults – Wireless - All vendor default settings on wireless equipment are changed.

Wireless Encryption Key - All wireless networks are configured to encrypt network communications using a long and complex Wi-Fi Protected Access 2 (WPA2) key.

Wireless Default Service Set Identifiers - All default service set identifiers (SSIDs) on wireless networks are changed. [KC13.5]

Wireless Encryption Configuration - All wireless networks are configured to encrypt network communications using the Wi-Fi Protected Access 2 (WPA2) certification with the Advanced Encryption Security (AES) algorithm. [KC13.5]

Domain Management

Internet Domain Name Registration - Payments and paperwork for internet domain name registrations for all Axio's official sites are handled in a timely manner and promptly confirmed by the Management Team.

Security for Domain Name Registrations - Axio consistently employs the most secure methods available for communicating with domain name registration authorities about Axio's web and commerce sites.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent

permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – 12.1.3 Capacity Management
ISO/IEC 27002:2013 – 13.1 Network Security Management
HIPAA Security Rule 164.312(a)(1): Access Control
HIPAA Security Rule 164.312(b): Audit Controls
AT 101-SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101-SOC 2: CC6.1 – Common Criteria related to System Operations
AT 101 - SOC 2: CC7.0 - Common Criteria Related to Change Management
AT 101 – SOC 2 – A1.1 to A1.3 – Additional Criteria for Availability

Axio Firewall Management Policy and Procedures

Purpose:	This policy defines the essential rules regarding the management and maintenance of firewalls and/or their equivalents in cloud environments referring to firewall rules and VPCs in GCP that allow for Axio to apply firewall rules restricting inbound and outbound traffic to the production systems.
Applies To:	This policy applies to all Axio firewalls (or systems performing the role of firewalls, such as routers, telecommunications front ends, and gateways). This applies to all firewall systems managed by employees or by third parties. Exceptions are permitted only if approved in advance and in writing by the COO.
Last Updated:	August 21, 2019

Please note: All references of "internal network" in this policy are to our instance of the GCP and the AWS for the platform. Axio currently does not have any internal networks or networked computer systems.

Business Justification and Selection

Standard Products - The production network relies on Native GCP firewall technology as a first layer of protection in the cloud. The GCP VPC, along with firewall rules functionality, represents the Axio-controlled layer of network protection within GCP. Kubernetes is used to manage the environment.

Client (or "Personal") Firewalls - All computers needing greater protection than what can be provided by firewalls closer to the edge of the network, as determined by due care or by a risk assessment, require implementation of a client (or "personal") firewall.

Firewall Dedicated Functionality - Team members connect directly to production through firewall protections maintained by GCP. Whenever freestanding firewalls (e.g., Cisco) are deployed, Axio operates the firewalls on dedicated machines that perform no other services, such as acting as a mail server. To the extent the supporting operating system allows it, all unnecessary and unused systems and network management software and services must be removed from company firewalls.

Required Documentation - Axio's COO maintains a network diagram and/or list of permissible paths and a description of permissible services, accompanied by a justification for each. [KC13.4]

Access Approval - Permission to enable communication paths and services is performed according to Axio's Infrastructure Change Management policy only when these paths or services are necessary for important business reasons, and sufficient security measures are consistently employed. The COO, and occasionally his designee, approve all firewall (when applicable) and/or production environment networking changes and access permission requests. Any changes to paths or services go through this same QA (where applicable) and approval process to enable access to Axio's infrastructure environment. [KC14.1]

Implementation

Connections Between Machines - Real-time connections between Axio's production environments with any external network are not to be established or enabled, which ensures that such direct connections do not unduly jeopardize information security. Firewalls or similar intermediate systems are employed to prevent direct connections. [KC14.1] This requirement applies regardless of the technology employed.

External Connections - All inbound real-time internet connections to Axio's systems or multiuser computer systems pass through a firewall equivalent. Axio's computer systems may be attached to the internet only when protected by a firewall.

Secured Subnets - Portions of Axio's internal network that contain critical or confidential data, such as the application and database servers, employ a secured subnet via Axio's management VPC. Indeed, the internal network IPs are screened to external devices. Based on periodic risk assessments, the Information Technology department redefines the secured subnets required in the information security architecture.

Demilitarized Zones - All internet facing servers are protected by firewall equivalents and are located within a demilitarized zone (DMZ), that is, a subnet that is protected from the internet by one or more firewall equivalents with restricted communication paths and types.

Additionally, firewalls are used to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a security group based on the system's function. VPC rules and firewall rules restrict access to only the ports and protocols required for a system's specific function to mitigate risk. [KC14.2]

Disclosure of Internal Network Information - The internal system addresses, configurations, products deployed, and related system design information for networked computer systems are restricted to preclude both systems and users outside the Axio internal network from accessing this information. Network address translation (NAT) is the preferred method for protecting internal IP addresses. Configuration and operation standards are implemented and maintained to preclude internal business information from being resident on or processed by any firewall, server, or other computer that is shared with another organization at an outsourcing facility.

Default to Denial - By default all access is denied and only explicitly allowed ports and protocols are allowed based on business need. At the GCP level, Google has mechanisms in place to protect its cloud infrastructure and its production services. These mechanisms are designed to ensure that no single service can overwhelm the shared infrastructure and to provide isolation among customers using the shared infrastructure. Axio applies the default deny principle by whitelisting necessary connections whenever possible and using VPC rules and firewall rules to restrict access to infrastructure resources. [KC14.3]

Firewall Access Mechanisms - All firewalls and their equivalents are configured with unique passwords or other access control mechanisms such as multifactor authentication to restrict the ability to make networking changes to only authorized Axio employees. Group user IDs are not allowed, and the same

password or access control code should not be used by more than one employee; unique user credentials are required, whenever possible.

Firewall Access Privileges - Privileges to modify the functionality, connectivity, and services supported by GCP native firewalls is restricted to GCP. Axio-controlled production network changes are made though Kubernetes only by authorized administrators. [KC14.1]

Firewall Physical Security - When a corporate network is established, and/or Axio-owned firewalls are deployed, all Axio firewalls outside of a secured data center will be located in locked rooms, closets, or cabinets that meet Axio's physical security standards and are accessible only to authorized firewall administrators. When firewalls are placed within a general data processing center, they are installed inside separately locked rooms, areas, cages, or racks.

Firewall Operation

Monitoring Vulnerabilities - GCP monitors and patches the Google firewalls, and Kubernetes is set to auto-patch the network systems. [KC14.5]

Firewall Logs - All firewalls and their equivalents are configured to log events according to the following standards for logging firewall activity:

- all changes to firewall (VPC and firewall rules) configuration parameters, enabled services, and permitted connectivity paths KC14.4
- all successful and failed access attempts into the Axio production environment [KC14.4]
- protection of the logs by checksums, digital signatures, and/or encryption
- prompt removal of the logs from the recording systems and storage in a physically protected area or container for at least six months
- periodic log review to ensure the secure operation of the firewalls or equivalents (see the Log Monitoring policy for specific controls and procedures)

GCP manages the configuration and settings of the firewalls protecting the GCP SaaS platform.

Change Management

Posting Updates - All changes made to the Axio infrastructure networking follows the Infrastructure Change Management P&P. Only authorized employees have access to the VPC portal used to establish and change Axio subnet rules. [KC14.1]

Firewall Monitoring

Periodic Review - GCP manages the firewall configurations. [KC14.7] Core production network configurations are reviewed every six months to ensure they are properly hardened. [KC 14.8]

Continuity Management

Secure Backup - Axio exports firewall rules to Stackdriver/Pub Sub to enable monitoring and analysis as needed. [KC14.6]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy should provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO 27002:2013 - 8.1.3 Acceptable use of assets
NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy, July 2008
HIPAA Security Rule 164.312(a)(1): Access Control
HIPAA Security Rule 164.312(b): Audit Controls
AT 101-SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101 - SOC 2: CC6.0 - Common Criteria Related to System Operations
AT 101 - SOC 2: CC7.0 - Common Criteria Related to Change Management
AT 101 – SOC 2 – A1.1 to A1.3 – Additional Criteria for Availability

Related Documents

Axio's Network Diagram

Axio Remote Access Management Policy and Procedures

Purpose:	This policy defines the requirements for establishing the framework and ongoing management of Axio's remote access infrastructure.
Applies To:	This policy applies to all remote access systems (i.e., servers, devices, and all things related) that are configured and implemented to remotely access any Axio computer or communications system. The target audience of this policy is all Axio employees who have production environment remote access management responsibilities or who have been given remote access to any Axio computer or communications system.
Last Updated:	August 21, 2019

Program Requirements

Remote Access Strategy Development - Prior to permitting or implementing any remote access to Axio's computer and communications systems, a detailed analysis is performed that includes an examination of the risks associated with each solution. No remote access into any Axio systems will be granted without authorization from the COO or their designees.

Remote Access Strategy Testing - Before implementing a remote access solution, a prototype of the design is tested and evaluated for security and performance compatibility.

Documentation and Process

Security Standard for Home User Computers - Axio's Mobile Device and Acceptable Use P&Ps within this ISP contain a standard for the security configuration of home computers, which employees use for remote access to Axio systems.

Integrated Remote Access Strategy - The security aspects of the remote access solution design are documented in Axio's system security plan. Specifically, VPN and two-factor authentication are implemented to access AWS and GCP production environment systems. [[KC15.1]

Annual Review of Information Security Policy Documents - All of Axio's written information security policy documents are reviewed on an annual basis by a team consisting (at a minimum) of members from the information security, legal, and human resource departments. [KC1.2]

Server Configuration

Remote Access Server Placement - Remote access servers are placed at the data center or cloud provider perimeter and must be configured under the principle of least privilege, with unnecessary ports and services disabled, active monitoring for potential intrusions, and periodic monitoring for potential vulnerabilities.

Authentication and Access

Two-Factor User Authentication - All inbound access through a public network to Axio's AWS production server employs two-factor user authentication, with at least one of the factors not subject to replay. [KC15.1]

Remote Access Passwords - Complex passwords are required to gain remote access into the corporate network. [KC15.2]

Privilege Restriction – Need to Know - The computer and communications system privileges of all users, systems, and programs are restricted based on the need to know. Services available to employees remotely are restricted based on their organizational role.

Semi-Annual Access Reviews - The computer and communications system privileges of all customer infrastructure systems (e.g., network, servers, and routers) and applications (e.g., databases and web applications) are audited annually to validate that terminated contractor and employee IDs have been disabled or, ideally, removed, and user privileges are commensurate with job responsibilities. [KC11.7]

Data Integrity

Confidential Data Transmission - All information deemed critical or confidential (see the Data Confidentiality Policy) by Axio that is transmitted over any communication network is encrypted. In particular, Axio employees with administrator privileges use VPN and/or another secured channel that encrypts the administrator ID authentication credentials when logging in remotely, thereby protecting confidential data from exposure to man-in-the middle and similar attack vectors. [KC15.1]

Standard Encryption Algorithm and Implementation - If encryption is used, Information Security Committee-approved standard algorithms [i.e., AES 256 or 3-DES] and standard implementations are consistently employed.

Server and Device Management

Remote Access Server and Device Security - For remote access servers controlled by Axio, remote access servers and devices are kept fully patched, operated using an organization-defined security configuration baseline, and are only managed from trusted hosts by authorized personnel. Axio monitors GCP alerts and industry resources for available security patches. Timely patching within 30 days is conducted on the infrastructure equipment. [KC15.3]

Remote Access Client Software Management - Remote access client software is configured to have all security features and settings remotely managed by a third-party system administrator.

Remote Access Client Device Support - Operations personnel are properly trained to support remote access users and the devices that are used.

Client Software

Remote Access Client Software Configuration - Remote access client software is configured to provide Axio with nearly complete control over the remote access environment.

Device Management and Security

Remote Access Device Management Training - All Axio employees who are responsible for the management of any remote access devices are trained to properly secure these devices.

Mobile Device Usage with Axio Information - All mobile computing devices used to conduct any Axio business is properly configured with necessary security software.

Remote Access Server and Device Security - All Axio's remote access servers and devices are kept fully patched, operated using an organization-defined security configuration baseline, and only managed from trusted hosts by authorized administrators. (See the Overview of Axio360 Technology and Security Architecture.)

Remote Client Machines Certificates Revoked If Lost/Stolen - Axio revokes, in a timely manner, remote and network access if a user is terminated or user equipment is lost or compromised. For terminated administrators who had remote access to the production servers, this is accomplished by disabling their access IDs and revoking the multifactor token. [KC15.4]

Data Security

Remote Server and Device Disposal - All critical and confidential data is removed from any remote server or device prior to its disposal. As detailed in the Information Disposal Policy, any hard drives that Axio maintains are sanitized in accordance with NIST 800-88 standards prior to disposal.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – 6.2.1 Mobile Device Policy
ISO/IEC 27002:2013 – 9 Access Control
HIPAA Security Rule 164.312(d) – Person or Entity Authentication
HIPAA Security Rule 164.312(e) – Transmission Security
PCI v3.1 Requirement 12.3
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 – SOC 2: CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls

AT 101 – SOC 2: CC4.0 Common Criteria Related to Common Criteria Related to Monitoring of Controls
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls

Axio Malicious Software Management Policy and Procedures

Purpose:	This policy defines the requirements for establishing the controls to prevent and detect the dissemination of any malicious software on Axio's computer and communications systems.
Applies To:	This policy applies to all Axio computer systems and facilities, with a target audience of Axio's Information Technology employees.
Last Updated:	August 21, 2019

Antivirus Deployment Installation

Antivirus Software Deployment - Antivirus software is deployed and executing on all Axio computer and communications systems commonly affected by malicious software (e.g., personal computers and servers) where applicable antivirus technology exists. Axio has implemented a web-based, centralized antivirus solution to protect user endpoints. [KC16.1] Based on Axio's research, antivirus is not necessary for the Google Cloud infrastructure that Axio runs.

Virus Software Installation - Virus screening software is installed and enabled on all Axio endpoints used by employees to perform work for Axio.

Kaspersky Products - Axio employees are *not* authorized to use Kaspersky products on Axio devices.

Antivirus Configuration

Antivirus Software Updates - All antivirus programs deployed on Axio's computer and communications systems are configured to accept automatic updates of the software and signature databases. [KC16.2]

Antivirus Software Scans - All antivirus programs deployed on Axio's computer and communications systems are configured to periodically scan the systems for viruses. [KC16.3]

Antivirus Software Logs - All antivirus programs deployed on Axio's computer and communications systems are configured to log all antivirus activity.

Virus-Checking Programs - Virus checking programs approved by the COO are continuously enabled on all networked personal computers and end-user devices used to conduct Axio business.

Malicious Software Program Access - Axio restricts the ability to disable or change the configuration to its antivirus software program to authorized personnel only.

Scanning

Regular Monitoring of Public-Facing Computers for Malicious Software - Production servers are monitored by the AWS Guard Duty intrusion prevention system, and Axio monitors and resolves all Guard

Duty alerts in a timely manner. All Axio end user devices are set to auto-scan periodically to perform a search for possible infection of malicious software. [KC16.3]

- Scanning Downloaded Software - All externally supplied computer-readable files are scanned for viruses prior to being loaded onto Axio's infrastructure. [KC16.4]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy should provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – 12.2.1 Controls Against Malware
AT 101 – SOC 2 – CC5.8 Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software
HIPAA Security Rule 164.308(a)(5)(ii)(B) – Protection from Malicious Software

Axio Log Management and Monitoring Policy and Procedures

Purpose:	This policy defines the requirements for managing and monitoring the logs that are generated by Axio's computer and communications systems.
Applies To:	This policy applies to all Axio computer and communications systems, with a target audience of Axio's Information Technology employees.
Last Updated:	August 21, 2019

Requirements

Security Logs - Security logs of an environment are captured in sufficient detail to allow for the detection and analysis of all common and current threats.

Operating System Logs - Operating system logs and application logs are recorded to capture security-related data.

Critical Application Logs - All critical business applications are supported by logs and audit trails. Google Cloud Monitoring and Stack Driver provide additional alerting and logging capabilities to alert management when system activity occurs that could impact the information security (confidentiality, integrity, and availability) of systems and/or data. System health and data throughput are analyzed through Google Cloud Monitoring. Axio captures login attempts and Assessment Module activities within its application, as well. [KC17.1]

Critical or Confidential Data Application Systems Logs - All production application systems that handle critical or confidential data generate logs that capture access information.

Critical or Confidential Data Access Logs - The identity of every user who accesses critical or confidential data resident on Axio's information systems is logged.

Systems Architecture for Logging Activities - Application and/or database management system software keeps logs of user activities, and statistics related to these activities, that in turn permit them to audit the logs and investigate suspicious business activities. Axio leverages Stackdriver and Pub Sub for log aggregation and analysis, as well.

Computer System Audit Logs - Logs of computer security-relevant events provide sufficient data to support comprehensive audits on the effectiveness of and compliance with security measures.

Privileged User ID Activity Logging - All user ID creation, deletion, and privilege change activity by system administrators within AWS is logged.

Production Change Reconstructability - All production application user activities affecting production information are fully reconstructible from logs.

Logging Logon Attempts - All user initiated failed logon attempts to connect with Axio's application and production information systems are logged. Axio captures login attempts and Assessment Module activities within the application. All Google Cloud platform API requests are logged, such as web requests, storage bucket access, and user account access attempts, as well. Finally, access into Kubernetes and changes made to the GCP environment using Kubernetes are also logged. [KC17.4]

Physical Access Logging - Axio's third-party data center providers maintain logs of all physical access, including electronic physical access systems, and visitor access recorded on paper. See the Physical Security P&P.

Log Composition

Event logs should record the following types of events including, but not limited to:

- user access
- user activities
- exceptions
- faults
- audit logs
- information security events
- changes to time settings on critical systems
- initialization of audit logs
- stopping or pausing of audit logs
- creation and deletion of system level objects

All logs should capture the following event information including, but not limited to:

- user ID
- date and time of login
- actions performed by the user
- date and time of actions performed by the user
- success and failure indications
- identity or name of affected data, system component, or resources

These user and device groups require logging:

- User operational and security activities are logged.
- Third-party user operational and security activities are logged.
- System administrator and operator operational and security activities are logged.
- Host and network device operational and security activities are logged.

Production Application System Log Contents - All computer systems running Axio's production application systems include logs that record, at a minimum, successful login to the application, user application session activity, failed logon attempts, logon date and time, and logoff date and time. At the application level, error handling logs, failed access attempts, and additional logging continue to be added as the application and end-user needs evolve. [KC17.3]

Password Logging - Unencrypted passwords, whether correctly typed or not, are never recorded in system logs.

Computer Operator Logs - All Axio's multiuser production systems have computer operator logs that show production application start and stop times, system boot and restart times, and system errors.

Monitoring

Log Review Frequency - The infrastructure monitoring and log tool alerts detailed above are reviewed using GCP, StackDriver, and Statuscake. [KC17.2] Alerts that require action by IT management are investigated and resolved in accordance with the Incident Response P&P.

Log Retention Period - Every log and audit trail produced by Axio computer and communications systems are retained for at least one year. At least three months of audit logs are available at all times for immediate analysis.

System Log Rotation and Archival - To prevent the overwriting of system logs or the expansion of these logs to the point where they consume all available disk space, a formal log rotation and archival storage process is in place for all network periphery security systems and all multiuser production servers.

Log Restoration - A process is in place to be able to restore at least the last three months of any log or audit trail produced by Axio computer and communications systems for immediate analysis.

Access

Systems Log and Audit Trail Disclosure - Systems logs and application audit trails are not disclosed to any person outside the team of individuals who ordinarily view such information to perform their jobs or investigate information security incidents. Axio restricts system log access to a limited number of authorized personnel.

Customer Activity Log Disclosure - Logs reflecting the activities of computer users or those served by computers are not disclosed to third parties unless Axio is compelled to do so by court order, law, or regulation, or in receipt of written approval from the involved individuals.

Clock Synchronization

All applications use their host system for time keeping. Time settings are restricted to only personnel with a business need to access time data. Production assets are configured to synchronize to trusted international time sources on a periodic basis.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 - 12.4.1 Event logging
AT 101 - SOC 2: CC2.0 – Common Criteria Related to Communications
AT 101 - SOC 2: CC3.0 – Common Criteria Related to Risk Management and Design & Implementation of Controls
AT 101 - SOC 2: CC4.0 – Common Criteria Related to Monitoring of Controls
AT 101 - SOC 2: CC5.0 – Common Criteria Related to Logical & Physical Access Controls
AT 101 - SOC 2: CC6.0 - Common Criteria Related to System Operations
HIPAA Security Rule 164.312(b) – Audit Controls
PCI DSS v3.1

Axio Backup and Recovery Policy and Procedures

Purpose:	This policy defines the requirements for maintaining and recovering backup copies of critical and confidential data created, processed, or stored on Axio's computer and communications systems.
Applies To:	This policy applies to server configurations and database backups that are housed on the GCP platform.
Last Updated:	August 21, 2019

Schedule

Data Backups - Axio applications deployed to the GCP platform are automatically backed up as part of the deployment process via Github's secure and access-controlled storage. MongoDB are backed up nightly to Google Buckets within GCP and are encrypted at rest. Snapshots are taken nightly via a Kubernetes script. Github is used for backing up the source code used by Axio. [KC18.1]

These backups are used to deploy Axio's applications across GCP's platform and to bring them back online in the event of an outage. Axio has set up alerts for failed backup investigations, and notifications are received via StackDriver. [KC18.2] Axio has a contract in place with GCP and Git (code) as their offsite backup storage vendor and the most recent backup rotation log. [KC18.7]

Configuration Backups - Production environment configuration backups are taken whenever configuration changes occur to support roll-back and are maintained in Git and/or within Kubernetes. [KC19.1]

Procedures

Off-Site Backup Files - At least one generation of backup files are maintained on offline data storage media wherever production computers are located.

Critical Backup Files - Critical data is backed up off-site based on the schedule defined by Axio. Critical data that has been backed up is not used for data restoration purposes unless another backup copy of the same data exists on different computer storage media. If this additional copy does not exist before the restoration, the copy must first be made on a computer other than the one where the restoration is to take place.

Website Archives - Every version of the internet website is securely archived.

Information Preservation After Application Decommission - Before any Axio product applications are taken out of production, a final backup of all critical and confidential production data is made and retained in a method and period dictated by the impacted customers. In the event that a customer decommissions without making arrangements with Axio for retention, all data is purged in accordance with the Confidential Data and Information Disposal Policies.

Business Continuity and Disaster Recovery - Axio does not have a physical presence with the exception of the Decatur, GA office. All Axio staff are able to work from any remote location. Axio maintains and updates, at least annually, its business continuity plan as part of its Disaster Recovery plan. [KC18.6] Disaster recovery tests of restores are performed to validate Axio's ability to recover from a disaster. [KC18.3]

Employee Laptops and Workstations – Normally, Axio employees store Axio data only in the Axio instance of Box. However, if for any reason Axio employees have stored Axio data on their laptops or workstations, they must back up their devices in accordance with the following:

- Weekly on-site backups
- Monthly off-site backups to either an online form or to a hard drive that is stored in a safe deposit box. The 1TB Microsoft OneDrive instance that each employee has can be used for this purpose.

Media

Backup Media Storage - Essential business information and software backups are stored in an environmentally protected and access-controlled site. Axio houses their production environment backups in commercial-grade data centers.

Retention Procedures - All backups are performed nightly, and backups are retained for a minimum of seven days. [KC18.4]

Archival Storage Directory - All archival backup data stored off-site is reflected in a current directory that shows the date when the information was most recently modified and the nature of the information.

Backup Media Encryption - Backup media are encrypted with Google Buckets. [KC18.5]

Testing and Review

Archival Storage Media Testing - Restores of nonfunctioning equipment are performed, as needed, from the functioning, replicated instance. [Key Control 18.3]

Archival Storage Media Quality - The computer data media used for storing critical and confidential data must be high quality and follows a cyclical (at least annual) testing schedule for backup integrity and reliability. [Key Control 18.3]

Backup Information Review - All files and messages stored on Axio systems are routinely copied to tape, disk, and other storage media and are recoverable for potential examination at a later date by system administrators and others designated by management.

References

ISO/IEC 27002:2013 - 12.3.1 Information backup
HIPAA 164.310(d)(2)(iv) – Data Backup and Storage
HIPAA 164.312(a)(2)(ii) – Emergency Access Procedures
HIPAA 164.308(a)(7)(i) – Contingency Plan
HIPAA 164.308(a)(7)(ii)(A) – Data Backup Plan

HIPAA 164.308(a)(7)(ii)(B) – Disaster Recovery Plan (Establish and implement procedures to restore any loss of data.)
AT 101 – SOC 2 – A1.1 to A1.3 – Additional Criteria for Availability

Axio Infrastructure Change Management Policy and Procedures

Purpose:	This policy defines the control requirements for the making hardware or software changes on Axio's infrastructure computer and communications systems.
Applies To:	This policy applies to all Axio computer systems and facilities, with a target audience of Axio's Information Technology employees and partners.
Last Updated:	August 21, 2019

Infrastructure Change Management Process

This policy covers changes required to routers, servers, firewalls, load balancers, database systems, backup tools, infrastructure monitoring tools, etc. Axio evidences infrastructure change management control execution in Axio's ticketing system for each change that could impact the information security (confidentiality, integrity, and availability) of customer data and/or systems and products. Application code changes are covered in the Code Change Management P&P. Configuration files are backed up by backup tool and by change owner prior to requesting infrastructure change to support roll-back. [KC19.1].

System administrators are responsible for monitoring and maintaining the customer application and data infrastructure [KC19.2]. Change request (CR) tickets are created for all infrastructure changes and patches. [KC19.9] A listing of all production system/infrastructure changes is maintained, including patches, virus, firewall, etc.

Axio's Infrastructure Change Control Protocol

1. The CR ticket is created for infrastructure change in the Axio ticketing system (Git), and if it is a change for which GCP is responsible, it is entered into the GCP ticket system.
2. Axio documents requirements within "Bugs" or "Management Story" within DevOps ticket. Whenever applicable, the change requestor documents all necessary steps for meeting the hardening baseline or references the security hardening guide to be applied in accordance with Axio's configuration hardening standard for that type of device, when applicable. [KC19.3]
3. When possible, CR adds acceptance criteria for every infrastructure ticket. For example, for server changes this is confirmation that the server matches the recipe for the server type, when applicable. [KC19.3]
4. Two approvals are required with at least one admin for all infrastructure change tickets. [KC19.4]
5. When applicable, Axio's account managers ensure that the clients are aware of any possible impact. [KC19.6]
6. Proposed infrastructure changes impacting employees are communicated in writing. [KC19.8]

Example of adequate testing per Axio's best practices:

- If this is a server change, the infrastructure change owner (ICO) (i.e., system administrator) confirms that the server matches the predefined hardening recipe.

- If this is a firewall change, the ICO confirms that all unused ports have been locked/disabled/masked and that all unnecessary services have been disabled.
- In order to continuously improve production environment information security (confidentiality, integrity, and availability), ICOs are encouraged to build hardening and testing templates, or at a minimum guidelines for each type of device in the production environment. [KC19.7]
- The ICO runs steps for user testing documented in the ticket or otherwise assesses the configuration against the hardening baseline and confirms that acceptance criteria are met.
- If the ICO or designee finds any issues, he/she describes them in a comment in the ticketing system for resolution by GCP. The ICO determines if the change needs to be rolled back.
- If no issues are found, testing results are noted in the ticket, and the ticket is closed.

Update Network Diagram (if necessary) - With each infrastructure change, the ticket owner works with the respective system administrators to update the network diagram, infrastructure schematics, and infrastructure inventory to ensure that the device is now monitored. [KC19.5]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – Access Control
PCI DSS 7, 8 & 9 – Restrict Access to CDE based on Need to Know; Identify and Authenticate Access & Restrict Physical Access to CDE
HIPAA Security Rule 164.312(e)(2)(i) – Integrity Controls
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101-SOC 2 – CC7 – Common Criteria Related to Change Management

Axio Code Changes Management Policy and Procedures

Purpose:	This policy defines the control requirements for making software changes on Axio's customer-servicing environments.
Applies To:	This policy applies to all Axio computer systems and facilities, with a target audience of Axio development employees and partners (if applicable).
Last Updated:	August 21, 2019

This policy details procedures and key controls specific to creating and updating application code for customer-servicing applications. See the separate Infrastructure Change Management P&P for hardware and related systems maintenance and installs, etc.

Project Stage

1. The process begins with a pull request ticket created in Axio's GitHub ticketing system to document the nature of the change and the core requirements and user acceptance criteria. [KC20.10]
2. The COO (or his designee) authorizes or denies the change request ticket.
3. Upon authorization, the ticket is assigned to a developer. [KC20.3]
4. The developer documents the basic requirements and validation testing to perform. [KC 20.2]

Development Environment Changes Stage

1. Axio has written code change management procedures to be followed by development. [KC20.1]
2. Once code is ready for the initial review, the change owner assigns an independent developer to perform the code review. It is then assigned to the QA team. If there are any issues, the ticket is then sent back to development for additional review. [KC20.4]
3. Upon successful code review, a change owner/lead developer tests the code, ensuring all the business requirements were met. Dev and QA are together in a single environment. [KC20.5]

Production Environment Changes Stage

1. Prior to the final move to production within the GCP environment, the COO or his designee reviews the ticket and supporting change documentation and validates that the business requirements were met and the code is executing as expected.
2. Snyk is used as the code vulnerability scanning tool, which is run prior to significant changes being pushed to production. NPM audits runs on build to look for non-secure code dependencies. [KC20.7]

Production Environment Testing

1. When a customer issue initiates the code change, Axio confirms with the customer, post-change, that the issue has been resolved and documents this confirmation in the ticket. [KC20.6]
2. In lieu of customer-acceptance testing, Axio performs user-acceptance testing within the production environment, as deemed necessary, to validate the efficacy of the changes. [KC20.6]

Segregation of Duties Controls

1. The final approval prior to pushing to production is made either by the COO or his designee, whoever did not request the change.
2. Likewise, developers do not have write access to production; only admins can deploy code into production. [KC20.8]

Confidentiality Control

1. Axio does not retain confidential information (e.g., user IDs, passwords) in its test environment. Any data pulled from the production environment is masked to prevent customer information exposure. There is no PII in the development environment. [KC20.9]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

AT 101 - SOC 2: CC7.0 - Common Criteria Related to Change Management
ISO/IEC 27002:2013 – 12.1.2 Change Management
ISO/IEC 27002:2013 – 12.1.4 Separation of Dev, Testing & Operational Environments
ISO/IEC 27002:2013 – 14.2 Security in Development & Support Processes

Axio Email Security Policy and Procedures

Purpose:	This policy provides the rules and requirements for the secure use and management of electronic mail. Each employee and contractor is required to acknowledge their understanding of and compliance with the comprehensive set of policies referred to as Axio's Information Security Policy upon hiring and annually. [KC1.1]
Applies To:	This policy applies to all users of Axio's information assets, including but not limited to Axio's employees, contractors, and partners. This policy applies whether electronic mail is accessed from Axio systems or via any remote location.
Last Updated:	August 21, 2019

Email Privileges

Authorized Usage - Axio's electronic communications systems generally have to be used for business activities only. Incidental personal use is permissible as long as it does not consume more than a trivial amount of system resources, does not interfere with worker productivity, and does not preempt any business activity. Axio's electronic communication systems are not used for charitable fund-raising campaigns, political advocacy efforts, religious efforts, private business activities, or personal amusement and entertainment. News feeds, electronic mail mailing lists, push data updates, and other mechanisms for receiving information over the internet are restricted to material that is clearly related to both Axio's business and the duties of the receiving workers. Workers are reminded that the use of corporate information system resources are never to create the appearance or the reality of inappropriate use. See the Acceptable Use P&P.

Default Privileges - Electronic communication systems are established and maintained such that only the privileges necessary to perform a job are granted to a worker. For example, when a worker's relationship with Axio comes to an end, all of the worker's privileges on Axio's electronic communications systems also cease. See the Access Control P&P for additional details.

User Separation - Where electronic communications systems provide the ability to separate the activities of different users, these facilities are implemented. For example, electronic mail systems employ personal user IDs and secret passwords to isolate the communications of different users. Unless a computerized fax mailbox system is employed, fax machines do not generally have separate mailboxes for different recipients, so such user separation is not required. Axio has established user separation; therefore, workers do not employ the user ID or the identifier of any other user. See the Account Management P&P.

Use at Your Own Risk - Workers access the internet with Axio's facilities at their own risk. Axio is not responsible for material viewed, downloaded, or received by users through the internet. Electronic mail systems may deliver unsolicited messages that contain offensive content.

Message Ownership

Company Property - As a productivity enhancement tool, Axio encourages the business use of electronic communications systems, notably the internet, telephone, voice mail, electronic mail, and fax. Unless third parties have clearly noted copyrights or some other rights on the messages handled by these electronic communications systems, all messages generated on Axio's electronic communications systems are considered to be the property of Axio.

No Guaranteed Message Privacy - Axio cannot guarantee that electronic communications are private. Workers are aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Electronic communications can be accessed by people other than the intended recipients in accordance with this policy. Because messages can be stored in backups, electronic communications may be retrievable when a traditional paper would have been discarded or destroyed. Accordingly, workers are careful about the topics covered in Axio's electronic communications and should not send a message discussing anything that they would not be comfortable reading about on the front page of their local newspaper.

Incidental Disclosure - It may be necessary for technical support personnel to review the content of an individual worker's communications during the course of problem resolution. These staff members do not review the content of an individual worker's communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels. Advance approval by the COO is required for all such monitoring.

Passwords

Sharing Passwords - Regardless of the circumstances, individual passwords are never to be shared or revealed to anyone else besides the authorized user. Information Technology Department staff will never ask users to reveal their passwords. If users need to share computer resident data, they should use public directories on local area network servers and other authorized information-sharing mechanisms.

Strong Passwords - To prevent unauthorized parties from obtaining access to electronic communications, users choose passwords that are difficult to guess. For example, users should not choose a dictionary word, details of their personal history, a common name, or a word that reflects work activities. See the Password P&P for specific requirements.

Multifactor Authentication (MFA) - To prevent unauthorized parties from performing brute-force password attacks on Axio email accounts, multifactor authentication is implemented through Office 365 that authenticates through Okta. [KC21.2]

Acceptable Use

User Identity - Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is forbidden. The username, electronic mail address, organizational affiliation, and related information included with electronic messages or postings reflect the actual originator of the messages or postings. All workers have the approved Axio email signature.

Use Only Axio Electronic Mail Systems - Axio employees are to use their provided axio.com accounts to conduct all Axio related business. Unless permission from the COO has first been obtained, workers should not use their personal electronic mail accounts with an internet service provider or any other third party for any Axio business messages.

Use of Encryption Programs - Axio's electronic communications systems are encrypted by default. These systems protect the critical or confidential data from end to end (from sender to recipient). [KC21.1] In other words, they do not involve decryption of the message content before the message reaches its intended final destination. See the Data Confidentiality P&P for additional details.

Email Content Restrictions

Respecting Intellectual Property Rights - Although the internet is an informal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. Workers using Axio's electronic mail systems can repost or reproduce material only after obtaining permission from the source, quote material from other sources only if these other sources are properly identified, and reveal internal Axio information on the internet only if the information has been officially approved for public release. All information acquired from the internet is considered suspect until confirmed by another source. There is no quality control process on the internet, and a considerable amount of information posted on the internet is outdated, inaccurate, and/or deliberately misleading.

Contents of Messages - Workers do not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. It is possible that these remarks would later be taken out of context and used against Axio. To prevent these problems, workers concentrate on business matters in Axio's electronic communications. As a matter of standard business practice, all Axio's electronic communications are consistent with conventional standards of ethical and polite conduct. Users are encouraged not to send user passwords, unprotected PANs (or other PCI data), or any data as defined by the Data Confidentiality Policy via messaging technologies (email, instant messaging, chat, etc.). [KC21.1]

Harassing or Offensive Materials - Axio's computer and communications systems are not intended to be used for and are not used for the exercise of Axio workers' right to free speech. These systems are not used as an open forum to discuss Axio's organizational changes or business policy matters. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Workers who receive offensive unsolicited material from outside sources should not forward or redistribute it to either internal or external parties, unless this forwarding or redistribution is to the Axio's COO in order to assist with the investigation of a complaint.

Email Attachments

Handling Attachments - When sending an attachment to a third party, workers attempt to use rich text format (RTF) or simple text files whenever possible. This is because attachments to electronic mail messages, if they have any executable code embedded in them, may contain a virus or may in some other way damage a worker's computer. Workers encourage third parties to send them files in these same two formats whenever reasonable and practical. All other attachment files are scanned with an authorized

virus detection software package before opening or execution. In some cases, attachments should be decrypted or decompressed before a virus scan takes place. Workers are cautious of unexpected electronic mail attachments received from third parties, even if the third party is known and trusted. Internet criminals are now able to remotely control machines and send viruses or other malicious electronic mail that seem to come from trusted sources. Many of the recent threats, as well as the common email risks, are covered in the annual security awareness training.

Message Forwarding - Electronic communications users exercise caution when forwarding messages. Axio's critical and confidential data is not forwarded to any party outside Axio without the prior approval of a local department manager. Blanket forwarding of messages to parties outside Axio is prohibited unless the prior permission of the COO has been obtained. Messages sent by outside parties are not forwarded to other third parties unless the sender clearly intended this and such forwarding is necessary to accomplish a customary business objective. In all other cases, forwarding of messages sent by outsiders to other third parties can be done only if the sender expressly agrees to this forwarding.

Handling Alerts About Security - Users promptly report all information security alerts, warnings, and reported vulnerabilities to the COO. Employees should familiarize themselves with the Incident Management P&P and the use of the Incident Response Report.

Reporting Phishing Attempts - If Axio workers receive an email that is clearly a phishing attempt, they forward it to phish@office365.microsoft.com as an attachment. (in Outlook, click on the email and then click Attachment in the Reply options group.) Axio subscribes to Advanced Threat Protection, which blocks many such emails, but some may get through.

Preventing Identity Theft

Responding to Unwanted Electronic Mail - If Axio's workers are bothered by an excessive number of unwanted messages from a particular organization or electronic mail address, they do not respond directly to the sender. Recipients forward samples of the messages to the system administrator in charge of the electronic mail system for resolution. Workers do not send large numbers of messages in order to overload a server or user's electronic mailbox in retaliation for any perceived issue.

Responding to Requests for Personal Information - Axio's workers should not respond to electronic mail messages that request personal information or critical or confidential company information, even from internal sources. These messages are most likely "phishing" attacks designed to steal such information. Axio's IT team will never request that you perform security duties, such as changing your password, via electronic mail. Any such requests are confirmed with separate communication from management.

Backup and Storage

User Backup - If an electronic mail message contains information relevant to the completion of a business transaction, contains potentially important reference information, or has value as evidence of an Axio management decision, it is retained for future reference. Users regularly move important information from online electronic mail message files to offline files (i.e., pst).

Axio Backup - Axio maintains copies of all email messages sent from or to axio.com accounts.

Purging Electronic Messages - Messages no longer needed for business purposes are periodically purged by users from their personal electronic message storage areas.

Employee Monitoring

Statistical Data - Consistent with generally accepted business practice, Axio collects statistical data about its electronic communication systems. For example, call detail reporting information collected by telephone switching systems records the numbers dialed, the duration of calls, the time of day when calls were placed, etc. Using such information, technical support personnel monitor the use of electronic communications to ensure the ongoing information security (confidentiality, integrity, and availability) of these systems. Axio employs computer systems that analyze these types of statistical information to detect unauthorized usage, toll fraud, denial of service attacks, and other problems.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 - 8.1.3 Acceptable Use of Assets
ISO/IEC 27002:2013 - 13.2.3 Electronic messaging
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls

Axio Mobile Device Management Security Policy

Purpose:	This policy defines the information security requirements for the protection of critical or confidential data on all Axio's mobile and portable computing devices. As outlined below, Axio establishes usage restrictions, configuration requirements, and implementation guidance for mobile devices. [KC22.1]
Applies To:	This policy applies to all Axio users who handle or are assigned tangible mobile computing, communications, or information assets belonging to Axio, including all employees, contractors, or temporary personnel.
Last Updated:	August 21, 2019

Configuration and Issuing of Mobile Devices

Approved Configuration of Mobile Computing Devices - Mobile computing devices, including personal digital assistants (PDAs), handheld computers, smartphones, flash drives, etc., are not be used to store Axio's business information unless they have been configured with the necessary controls and approved for such use by the COO. Further, customer confidential information (e.g., PII) should never be stored on mobile computing devices in accordance with the Confidential Data Policy. If data must be stored locally, the device drive must be encrypted at rest.

As noted throughout the ISP, all devices used for Axio's business are to [KC22.2]

- be enabled for auto-security patching on their specific operating system
- have company-provided, active antivirus/antimalware with auto-update and auto-scanning enabled

Verification of Approved Mobile Computing Devices - Workers do not use mobile devices to process any of Axio's information that is not classified as publicly available until the requirements for security operation have been met and verified (e.g., encryption at rest enabled).

Mobile Device Security Awareness Training - Because of the unique risks to mobile computing devices, all Axio employees who use mobile computing devices receive specific training on the risks of mobile computing and on the contents of this Mobile Device Security Policy. This is covered annually during the Security Awareness Training.

Bluetooth Devices Disabled by Default - All personal wireless-enabled devices, including cellular phones and PDAs, have default security settings that prohibit automatic discovery of networks. Bluetooth, Wi-Fi, infrared, and other wireless interfaces are disabled until they are specifically needed. If needed for some purpose, the Bluetooth wireless interface should be set in discoverable mode only temporarily, until pairing with another device is completed.

Service Limits for Mobile Phones - All cellular phone service agreements adopted by Axio limit the functionality of mobile devices to a minimum, standard service configuration defined by the COO.

Mobile Computing Configuration and Data Management

Approval for Storage of Critical or Confidential Data on Mobile Devices - All mobile computing devices used to conduct any Axio business are approved by the COO or his designee for use with the information appropriate for the normal business activities of the individual user.

Ownership of Information Stored in Mobile Devices - Axio allows members of its workforce to use mobile computing equipment so that they can perform their jobs at remote locations including hotel rooms and personal residences. The information stored in any portable computer equipment used for Axio's business is Axio's property and can be inspected or used in any manner at any time by Axio. Axio retains the right to wipe clean any and all company data at the time workers are no longer employed by Axio.

Storage and Labeling of Portable Media - Axio's policy is that portable media like USB drives or even hardcopies should not be used or produced with customer information in or on them. All customer and Axio critical or confidential data remains on the infrastructure servers and accessed only via VPN or other encrypted transport protocol and requires a second-factor authentication token to be provided. If there is ever a need to transport critical or confidential data, COO approval is obtained. When critical or confidential data is written to a portable storage device such as a portable disk, smart card, or other storage media, the media is suitably marked with the highest relevant classification and encrypted. FileVault and Jamf are used if the need arises for remote wiping or remote lock for laptops. [KC22.3]

Storage of Remote Access Information in Portable Computers - Users do not store remote access information (such as fixed passwords and user IDs) in their portable computer, or the case it is kept or carried in, because this could allow a thief to readily gain unauthorized access to Axio's networks.

Lending Computing Equipment Containing Critical or Confidential Data - A personal computer, handheld computer, transportable computer, personal digital assistant, smartphone, or any other computer used for business activities that contains Axio critical or confidential data is not to be loaned out to anyone.

Downloaded Software on PDAs, Smartphones, and Other Hybrid Devices - If personal digital assistants or smartphones are used for Axio's business activities other than voice conversations and/or meeting scheduling, do not download and install any software for the device.

Changes to Configurations and Software - On Axio's supplied computer hardware, workers do not change the operating system configuration or install new software. If such changes are required, they are performed by authorized personnel with remote system maintenance software. Changing the font defaults for a word processing program, or otherwise altering the templates provided with an application, is permissible without IT team assistance or advance approval.

Teleworking

Axio Property at Alternative Work Sites - The security of Axio's property at an alternative work site is just as important as it is at the central office. At alternative work sites, reasonable and prudent precautions are taken to protect Axio's hardware, software, and information from theft, damage, and misuse.

Alternative Work Site Requirements for Teleworkers - Before a telecommuting arrangement can begin, the worker's supervisor or manager should be satisfied that an alternative work site is appropriate for the Axio work performed by the involved worker.

Approved Teleworker Equipment - Employees working on Axio's business at alternative work sites use Axio-provided computer and network equipment, unless other equipment has been approved by the COO or his designee as compatible with Axio's information systems and controls.

Personally Owned Computer Systems - Workers do not use their own mobile computing devices, computers, computer peripherals, or computer software for Axio's teleworking business without prior authorization from their supervisor.

Lockable, Burglar-Resistant Furniture - All workers who keep critical or confidential data and mobile devices at their homes to perform their work, receive from Axio or otherwise provide approved lockable cabinets or desks for the proper storage of this information.

Telecommuter Information Security Procedures - Telecommuters follow all remote system security policies and procedures including, but not limited to, compliance with software license agreements, performance of regular backups, hard disk encryption packages, locking file cabinets, and use of shredders to dispose of critical or confidential paper-resident data.

Telework Space Environmental Controls - Equipment should be located and/or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.

Physical Security Protection

Personnel Responsibility - All mobile devices in the possession of company personnel are to be protected from physical threats such as loss due to theft or vandalism. Each employee must help ensure that their mobile devices used for Axio work are physically protected at all times.

Locking Personal Offices or Conference Rooms - All workers with separate personal offices should lock the doors when these offices are not in use or otherwise unattended.

Leaving Mobile Devices Unattended - Workers keep Axio's portable computers containing Axio information in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe.

Mobile Devices Stored Out of Sight - All portable devices in the possession of Axio personnel are stored in a secure location, such as a locked file cabinet or drawer, when not in use. Under no circumstances should portable devices be left in open view on desks or in public areas.

Authentication and Network Access

Wireless Network Connection Authentication - Wireless networks implemented by Axio must use WPA 2 strength encryption, at a minimum, and all users must be authenticated prior to granting access.

Axio employees must protect any mobile device used to process Axio data with a minimum of a six-digit PIN and/or a biometric authentication control.

Separate Password for Portable Devices - Axio's workers must not use the same password for a handheld device that is used for network (i.e., infrastructure) access or for access to other devices and applications. Different techniques exist to recover the password from various handheld devices, which in turn could possibly compromise access to the network or other devices.

Removal of Devices or Equipment

Required Authorization - Equipment, information, or software should not be taken off-site without prior authorization.

Storage Media Removal - All computer storage media leaving Axio's offices must be encrypted and are approved by the COO [KC22.4].

Travel Considerations

Removal of Critical and Confidential Data - Critical and confidential data may not be removed from Axio's premises unless the data owner and the COO have approved in advance. This policy includes critical or confidential data stored on portable computer hard disks, USB drives, CD-ROMs, magnetic tape cartridges, and paper memos. An exception is made for authorized off-site backups that are in encrypted form.

Checked Luggage - Workers in the possession of laptops, notebooks, tablets, handhelds, smartphones, personal digital assistants, and other portable computers containing critical or confidential Axio data are not to check these computers in airline luggage systems. These computers should remain in the possession of the traveler as hand luggage.

Bluetooth - Workers turn off Bluetooth on mobile devices when traveling whenever it is not needed.

Foreign Transport of Critical or Confidential Data - Whenever critical or confidential data is carried by an Axio worker into a foreign country, the information is either stored in some inaccessible form, such as an encrypted external storage media, or remains in the worker's possession at all times. Axio's workers shall not take critical or confidential Axio data into another country unless permission has been obtained from the data owner and COO.

International Travel - All of Axio's employees traveling with critical or confidential data must take special precautions when traveling overseas. Mobile devices should be stripped of all non-essential information and functionality and employ both full-disk encryption and two-factor authentication, if feasible. When traveling to high-risk areas, Axio employees should consult with senior managers about which devices and accounts are authorized for use. Alternative email accounts, temporary laptops (i.e., laptops that are wiped after travel has ended), and other measures should be used as senior managers judge necessary depending on the location and purpose of the travel.

Inspection of Machines for International Travel - All Axio personnel returning from overseas travel to any countries or regions on the US "Do Not Travel" list or other high-risk areas should have their laptops and other portable devices inspected by the COO or his designee before connecting to the Axio network. This inspection is required to check for malicious software or other security vulnerabilities that may have been introduced during inspection by authorities.

Lost or Stolen Mobile Devices

Immediate Reporting of Lost Devices - All Axio personnel are required to immediately report lost or stolen mobile devices to both their immediate supervisor and the IT Department. Such events are

escalated to the COO as necessary. Additionally, an Incident Response Report is completed in accordance with the Incident Response P&P.

Return and Decommission of Mobile Devices

Mobile Devices Are Returned for Decommission - All Axio-issued mobile devices, including laptops, PDAs, and cell phones are returned to Axio when no longer in use by employees or contractors. Under no circumstances should employees dispose of mobile devices that contained critical or confidential Axio or customer data.

Information Removal Before Disposal - Before disposal, donation, or recycling, the COO or his designee validates that critical and confidential data has been removed from any information systems equipment that has been used for Axio business. This validation process takes place before releasing such equipment to a third party.

Return of Property at Employment Termination - At the time that every employee, consultant, or contractor terminates his or her relationship with Axio, all Axio property including, but not limited to, portable computers, library books, documentation, building keys, magnetic access cards, credit cards, and outstanding loans, are to be returned. These terminating individuals inform management about all Axio property they possess, as well as all computer system privileges, building access privileges, and other privileges that they have been granted.

Inventory of Decommissioned Portable Equipment - The COO or his designee maintain an inventory of Axio's portable computer and network equipment and completes chain of custody forms for any device that has been taken out of commission. The inventory and chain of custody forms must reflect all actions taken to clear memory chips, hard drives, and other storage locations in this same equipment of all stored information.

Mobile Devices Not to Be Resold - Axio does not resell or recycle any mobile devices that contained critical or confidential Axio or customer data. These devices are destroyed using procedures approved by the COO.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO 27002 - 11.7 Mobile Computing and Teleworking

Axio Incident Response Policy and Procedures

Purpose:	This policy is intended to ensure that the company is prepared if a security incident were to occur. It details exactly what occurs if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice and approaches the topic from a security practices perspective.
Applies To:	This policy applies to all Axio employees and contractors. The scope of this policy covers all information assets owned or provided by the company, whether they reside at Axio's facilities or elsewhere.
Last Updated:	August 21, 2019

Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out incident response policy is critical to successful recovery from an incident. This policy covers all incidents that may affect the security and integrity of the company's information assets and outlines steps to take in the event of an incident.

Axio developed its Incident Response Policy based on ISO/IEC 27035:2011 "Information technology -- Security techniques -- Information security incident management."

Axio employees must take necessary steps to mitigate security violations in a timely manner and seek assistance whenever unsure about what to do or how to respond.

Types of Incidents

A security incident, as it relates to the company's information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

- Electronic: This type includes incidents such as an attacker or user accessing the network for unauthorized or malicious purposes, a virus outbreak, a suspected Trojan, and a malware infection.
- Physical: A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA, smartphone, portable storage device, or other digital apparatus that may contain company information.

Confidentiality

All information related to an electronic or physical security incident is to be treated as confidential information until the incident is fully contained. This serves both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness) and to control the release of information to the media and/or customers.

Preparation

Work done prior to a security incident is as important as work done after an incident is discovered. Axio performs an annual risk assessment focusing not only on risks to its annual strategic business objectives but also risks specific to information technology and fraud and other illegal acts. [KC23.1] Likewise, Axio prioritizes its information technology assets as part of its Infrastructure architecture mapping and the ITGCs implemented to protect its and clients' infrastructure. Finally, management uses logging and alerts to monitor for unauthorized access attempts into the Axio infrastructure. [KC23.3]

As part of the annual Security Awareness Training, Axio reiterates the procedures to ensure that the following is clear to all personnel:

- What actions to take when an incident is suspected
- Who is responsible for responding to an incident
- How the Security Incident Report is used for physical and electronic security incidents

Axio employees are required to read and acknowledge the Incident Response Policy. [KC23.2] The company has several security firm contacts to be used when expert resources are needed, and management stays abreast of industry and governmental regulations that dictate how Axio responds to a security incident (specifically, loss of customer data) and ensures that its incident response plans adhere to these regulations.

Finally, as noted in the Risk Management P&P, Axio is continuously monitoring GPC, US-CERT, and other vendor alerts for vulnerabilities and available security patches. Likewise, Axio runs routine (at least annual) vulnerability scans against the production environment.

Management's guidelines for the timely remediation of vulnerabilities are as follows:

Vulnerability Rating (CVE or Equivalent)	Time to Remediate in Production
Critical	15 Days
High	30 Days
Medium	60 Days
Low	180 Days

Incident Classification

To ensure the proper handling of security incidents, Axio has developed the following matrix to assist those responsible for handling incidents in determining the severity level of an incident and the communication protocol to follow.

Incident Factors	Priority Characteristics			
	Low	Medium	High	Urgent
Criticality – Application	No customer impact; no critical or confidential data at risk	Little/some customer impact but low risk of worsening in 24 hours	Multiple customers impacted or critical application at risk	Business operations impacted across customers or critical app unresponsive for > 30 minutes
Criticality – Infrastructure	No customer impact; no critical or confidential data at risk	Little/some customer impact but low risk of worsening in 24 hours	Multiple customers impacted or critical infrastructure system at risk	Business operations impacted across customers or critical architecture down for > 30 minutes
Impact – Public	None	Potential impact	Likely impact	Definite impact
Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures	No countermeasures
Escalation Required (done by Dan or Dale)	No	No	Yes – Dave (at a minimum)	Yes – Dave (at a minimum)

Electronic Incidents

When an electronic incident is suspected, the company's goal is to recover as quickly as possible, limit the damage done, and secure the network.

Axio proactively monitors for security breach attempts at the network level and at the core infrastructure device level.

- Network Level: The Google Cloud Platform Docker containers that support the platform are actively monitored for unauthorized access attempts, and Axio reviews logs as needed. [KC17.1]
- Database Level: The Google Cloud Platform Docker containers that support the platform are actively monitored for unauthorized access attempts, and Axio reviews logs as needed. [KC17.1]
- Server Level: The Google Cloud Platform Docker containers that support the platform are actively monitored for unauthorized access attempts, and Axio reviews logs as needed. [KC17.1]

Eradicating Computer Viruses - Any user who suspects infection by a virus should immediately disconnect from all systems, call Dan Hirt (for Axio endpoints) or Dale (for the platform), and make no attempt to eradicate the virus.

Electronic Incident Response

Once an actual or suspected incident has been reported by a user, the following steps should be taken in order by Dan or Dale:

1. Confirm that a security incident is occurring or has occurred.

2. Use the incident classification matrix to determine the severity of the incident and escalate as indicated by the severity level.
3. If the system can be isolated without interrupting business operations, remove the compromised device from the network by unplugging or disabling the network connection. Incidents involving mission-critical devices that cannot be isolated must be monitored closely, particularly the network activity in and around the device. Security personnel and management must discern in real time if the device should be taken offline.
4. Do not power down the machine.
5. Disable the compromised account(s) as appropriate.
6. The COO or CPO notifies law enforcement if needed.
7. Use the Security Incident Report Form template in Business-Operations/Incident Response to create a new security incident report to log the incident. Immediately do a Save As and save the file in a folder in the Incident Response folder named yyyy-mm-dd-<descriptor>, where <descriptor> is a three or four word description of the event. Name the report file yyyy-mm-dd-Security-Incident-Report-vx. Save to a new version each time the file is updated.
8. Copy/image the machine to another system and back up all data and logs on the machine. No forensic work should be performed on the original equipment.
9. Root cause analysis, if deemed to be necessary: Using all available system logs that were imaged/backed up, determine exactly what happened and the scope of the incident. Was it an accident, an attack, a virus? Was confidential data involved? Was it limited to only the system in question or was it more widespread? (This may be done by an external resource.)
10. The COO or CPO contacts an IT security consultant if needed.
11. Determine how the attacker gained access and disable this access.
12. Rebuild the system, including a complete operating system reinstall.
13. Restore any needed data from the last known good backup and put the system back online.
14. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) do not reappear.
15. Reflect on the incident. What can be learned? Was the policy adequate? What could be done differently? Document the lessons learned and remediation taken on the Security Incident Response form. Close the ticket. [KC23.4]
16. Consider a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.
17. Close the report once approval has occurred.

Physical Incidents

Physical security incidents are challenging, since often the only actions that can be taken to mitigate them should be done in advance. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable policies, such as those covering encryption and confidential data, should also be reviewed.

Physical security incidents are most likely the result of a random theft or inadvertent loss by a user, but they are treated as if they were targeted at the company.

The company assumes that such a loss will occur at some point, and periodically surveys a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

Physical Incident Response

Once an actual or suspected incident has been reported by a user, the following steps should be taken in order by Dan or Dale:

1. Use the incident classification matrix to determine the severity of the incident and escalate as indicated by the severity level.
2. Determine what kind of data was stored on the missing device. This can often be done by referring to a recent backup of the device. Three important questions must be answered:
    a. Was critical or confidential data involved?
        i. If not, refer to “Loss Contained” below.
        ii. If it was, refer to “Data Loss Suspected” below.
    b. Was strong encryption used?
        i. If it was, refer to “Loss Contained” below.
        ii. If not, refer to “Data Loss Suspected” below.
    c. Was equipment with VPN access to client infrastructure lost?
        i. If not, refer to “Loss Contained” below.
3. Use the Security Incident Report Form template in Business-Operations/Incident Response to create a new security incident report to log the incident. Immediately do a Save As and save the file in a folder in the Incident Response folder named yyyy-mm-dd-<descriptor>, where <descriptor> is a three or four word description of the event. Name the report file yyyy-mm-dd-Security-Incident-Report-vx. Save to a new version each time the file is updated. [KC23.4].
4. Close the report once approval has occurred.

Loss Contained

First, change any usernames, passwords, account information, encryption keys, passphrases, etc. that were stored on the system. Notify the COO or his delegate. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

Data Loss Suspected

Notify the Executive Management team to understand the company exposure and engage each relevant team to evaluate and prepare a response in their area. Change any usernames, passwords, account information, encryption keys, passphrases, etc. that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls. [KC23.4]

Notification

If an electronic or physical security incident is suspected to have resulted in the loss of third-party/customer data, Axio notifies the public or affected entities.

First this is discussed with the Executive Management team to determine an appropriate course of action. If notification is deemed an appropriate and/or legally required, it should occur in an organized and consistent manner. In addition, security incidents requiring system downtime and/or significant system

changes would be communicated at a customer's request. [KC23.5] (Axio's EULA does not specify that customers will be notified about system downtimes.)

Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies, such as the Risk Management P&P, relate to the topics covered in this document and should be reviewed as needed.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

AT 101 – SOC 2: CC1.0. Common Criteria Related to Organization and Management
AT 101 – SOC 2: CC3.0 Common Criteria Related to Risk Management and Design and Implementation of Controls
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101- SOC2: CC6.0 Common Criteria related to System Operations
AT 101- SOC2: CC4.1 Common Criteria Related to Monitoring of Controls
HIPAA Security Rule 164.308(a)(7)(ii)(E): Applications and Data Criticality Analysis
HIPAA Security Rule 164.312(b): Audit Controls
HIPAA Security Rule 164.308(a)(8): Evaluation
ISO/IEC 27002:2013 – 12.4 Logging & Monitoring
ISO/IEC 27002:2013 – 161 Information Security Incident Management

Axio Acceptable Use Policy and Procedures

Purpose:	This policy defines the activities that are permissible when using Axio computer and communications systems. At employment and annually, Axio enforces acknowledgement by every employee and contractor of the understanding and adherence to this policy. [KC24.1]
Applies To:	This policy applies to all users of Axio's computer and communications systems and information assets, including but not limited to Axio employees and partners.
Last Updated:	August 21, 2019

User IDs and Passwords

Personal User IDs – Responsibility - Users are responsible for all activity performed with their personal user IDs. They do not permit others to perform any activity with their user IDs, and they do not perform any activity with IDs belonging to other users. Axio ensures that all employees and contractors are assigned unique user IDs. [KC24.2]

Where shared IDs are required to be used to access customer infrastructure environment, management limits authorized personnel who can access. [KC11.3]

Access Code Sharing - Axio's computer accounts, user IDs, passwords, and any other access codes are not used by anyone other than the person to whom they were originally issued [KC24.3]

Script Files on Laptops, Tablets, and Smartphones - Users do not store clear-text authentication credentials on laptops, tablets, or smartphones, and never set up or employ script files that contain a stored version of a personal identification number (PIN) or a password that can be used to gain access to an Axio information system. Likewise, these security parameters should never be stored anywhere on these devices unless they are in encrypted form.

Typing Passwords When Others Are Watching - Workers never type their passwords at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.

Password Structure - Workers do not employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of user IDs, common character sequences, personal details, or any part of speech. See Password P&P.

Suspected Password Disclosure – A user immediately changes his or her password if the password is suspected of being disclosed or known to have been disclosed to an unauthorized party.

Password Proximity to Access Devices - Users never write down or otherwise record a readable password and store it near the access device to which it pertains.

Passwords in Communications Software - Users do not store fixed passwords in dial-up communications programs, internet browsers, or related data communications software at any time.

Electronic Messaging

(See Email Policy)

Reasonable Personal Use of Computer and Communications Systems - Axio allows computer users to make reasonable personal use of its electronic mail and other computer and communications systems. All such personal use is consistent with conventional standards of ethical and polite conduct.

Permissible Uses of Instant Messaging Facilities - Axio's approved instant messaging (IM) facilities may be used for collaboration and coordination only. Contractually binding agreements, as well as critical or confidential data, is sent through other communication channels.

Internet and Intranet

Forwarding Intranet Information - Workers do not forward information appearing on the intranet to third parties without first obtaining approval from the Axio data owner. (Axio does not currently have an intranet.)

Functional Manager Approval for Internet Software Downloads - Before end users download any software from the internet, run such software on any Axio computer, and/or use such software with any Axio business information, they first obtain their functional manager's written approval of the involved software license agreement. Before providing this approval, a department manager fully understands the functionality of the software and consults with the Information Technology team, and also determines that the software is fully compliant with Axio's information security requirements. [KC24.4]

Internet Discussion Groups - Users are not to post to controversial discussion groups on the internet or to any other controversial online public forums when using their Axio user IDs.

Internet Product and Service Representations - Workers are not to advertise, promote, present, or otherwise make statements about Axio's products and services in internet forums such as mailing lists, news groups, or chat sessions without the prior approval of the COO.

Uploading Software - Users are not to upload software that has been licensed from a third party, or software that has been developed by Axio, to any computer through the internet unless authorization from the user's manager has first been obtained.

Public Electronic Forums - Workers are not to use Axio's information systems to participate in internet discussion groups, chat rooms, or other public electronic forums unless this participation is expressly authorized by the COO.

Personal Internet Service Provider Accounts - Workers who wish to make a statement in a public internet forum about any topic that does not involve Axio's business, or Axio's business interests, use their own personal internet service provider accounts to submit such statements.

Personal Use of Internet - Use of Axio's information systems to access the internet for personal purposes will not be tolerated and may be considered cause for disciplinary action up to and including termination.

All users of the internet should be aware that firewalls can create a detailed audit log reflecting transmissions, both inbound and outbound.

Internet Connection Approval - Workers are not to establish any external network connections that could permit non-Axio users to gain access to Axio's systems and information, unless prior approval of the Information Technology Department has first been obtained.

Large Internet Downloads - Internet users are not to use video streaming facilities or audio streaming facilities or download large graphics files unless these transmissions are approved in advance by the user's immediate supervisor.

Critical or Confidential Data Not Accessed from Public Terminals - Employees do not use public web terminals to access critical or confidential Axio data. (See Remote Access Security P&P.)

Unencrypted Personal Identifiers Sent Via Internet Prohibited - Workers never transmit any personally identifiable information (such as Social Security numbers and birth dates) unencrypted over the internet. This prohibition includes email, instant messaging, chat rooms, and other communication systems.

Internal Systems

Please note: "Internal Systems" in this section refers to Axio-issued computers using Axio-issued and other software. Axio currently does not have any internal networks or networked computer systems.

Involvement with Computer Viruses - Users do not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Axio computer.

Eradicating Computer Viruses - Any user who suspects infection by a virus should immediately disconnect from all systems, call Dan Hirt (for Axio endpoints) or Dale (for the platform), and make no attempt to eradicate the virus.

Software Scanning – For Axio endpoints, the COO maintains authorized list of approved applications. [KC24.4] All permitted software downloads are scanned by the Axio malware scanning tools in place for end users.

Hacking Activities - Workers do not use Axio's information systems to engage in hacking activities that include but are not limited to (a) gaining unauthorized access to any other information systems, (b) damaging, altering, or disrupting the operations of any other information systems, and (c) capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.

Circumventing Access Controls - Programmers and other technically oriented staff refrain from installing any code that circumvents the authorized access control mechanisms found in operating systems or access control packages.

Testing Information System Controls - Workers do not test or attempt to compromise internal controls unless this activity is specifically approved in advance, and in writing, by the COO.

Encryption Usage Aside from That in Browsers - Aside from the encryption that is built into internet browsers, users do not employ encryption of any sort when using computer systems or networks unless these encryption systems have first been established and approved by the COO.

Prohibition Against All Forms of Adult Content - All forms of adult content (pornography or what some would consider pornography) are prohibited on Axio's computers and networks. This includes content obtained via websites, email attachments, CD-ROMs, and file sharing networks.

Discussions Using Computer and Communications Facilities - Axio's internal computer and communications systems (voice mail systems, electronic bulletin boards, database management systems, electronic mail facilities, intranet sites, etc.) are not used as an open forum to discuss Axio's organizational changes or business policy matters.

Program Resource Consumption - Computer users do not run or write any computer program or process that is likely to consume significant system resources or otherwise interfere with Axio's business activities.

Software Duplication - Users do not copy software provided by Axio to any storage media, transfer such software to another computer, or disclose such software to outside parties without written permission from the COO.

Unauthorized Software and Data Copies - Axio strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If system users make unauthorized copies of software, the users are doing so on their own behalf, since all such copying is strictly forbidden by Axio. Likewise, Axio allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

Equipment

Users are Responsible for Laptop Security - Users are required to ensure that all system and application patches are kept up-to-date. Likewise, users are required to ensure that antivirus patches and system scans are up-to-date and performed in accordance with the Malicious Software P&P. [KC22.2]

User Installation of Software - Axio employees have local administrative privileges but use those privileges only when absolutely necessary for maintaining the device. Users should only download and install software on their personal computers that is necessary for Axio business.

Sharing a Personal Computer with Other People Prohibited - Workers do not share their personal computer, if it is used for Axio business, with any other person. [KC24.3]

An exception may be made in cases where a personal computer has been configured so that separate user IDs and privilege profiles are supported for each separate user. Each such case must be approved by the Information Technology Department.

Unattended Active Sessions - If the computer system to which they are connected or which they are using contains critical or confidential data, users do not leave their personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

Accepting Security Assistance from Outsiders - Users do not accept any form of assistance to improve the security of their computers without first having the provider of this assistance approved by the Axio

Information Technology Department. This means that users are not to accept offers of free consulting services, not to download free security software via the internet, and not to employ free security posture evaluation web pages, unless the specific provider of the assistance has been previously approved.

Games on Organization Computer Systems - Games may not be stored or used on any Axio computer systems.

Modem Line Registry - Workers are not to install or contract for the installation of modem or similar lines unless they have been approved by the Information Technology Department.

Critical or Confidential Information on Transportable Computers - Workers possessing a portable, laptop, notebook, handheld, or other transportable computer containing critical or confidential Axio data should not leave these devices unattended at any time unless the data contained therein is exclusively stored in encrypted form.

Transportable Computers on Airplanes - When traveling by air with a portable electronic device containing critical or confidential Axio data, workers should not check these computers in airline luggage systems.

Lending Computers Containing Critical or Confidential Data - A personal computer or device used for business activities that contains critical or confidential data are not be lent to anyone.

Security of Mobile Devices When Traveling - Users should keep all mobile devices out of sight and locked up when stored in an unattended hotel room. Mobile devices containing Axio-related data should not be placed in the trunk of a taxi or other transport service (e.g., Uber) vehicle.

Physical Protection of Wireless Handheld Devices and Network Interface Cards - Wireless handheld devices, and any other devices containing wireless network interface cards (NICs), are physically protected by the user from loss, theft, and tampering. To maintain access control to Axio data, any loss, theft, or tampering of these devices is immediately reported to the Slack access channel.

Telephones and Voice Mail

Critical or Confidential Data on Answering Machines - Workers do not record messages containing critical or confidential data on answering machines or voice mail systems.

Voice Mail Message Storage - Unless they are on vacation or sick leave, users should check their voice mail at least once every business day.

Securing Information

Storing Mixed Classified Information - Axio workers do not store critical or confidential data with non-critical or non-confidential data on removable data storage media.

Storage of Critical or Confidential Information - Axio workers do not store critical or confidential data on personal computer or workstation hard disk drives unless the Information Technology Department has determined that adequate information security measures are employed.

Disclosing Customer Business Information - Axio workers do not disclose to anyone outside Axio the nature of customer projects, customer business strategies, or customer business relationships.

Disclosure of Third-Party Information - Axio workers do not disclose critical or confidential data that has been entrusted to Axio by third parties to other third parties unless the originator of the information has provided advance approval of the disclosure and the receiving party has signed an approved non-disclosure agreement.

Trade Secret Disclosure - Workers diligently protect from unauthorized disclosure all Axio information specifically identified as trade secrets. Trade secrets are identified as such prior to being disclosed to any workers.

Copying Critical or Confidential Data - Making additional copies of or printing of extra copies of critical or confidential data does not take place without the advance permission of the information owner.

Securing Critical or Confidential Data - Workers in custody of Axio critical or confidential data take appropriate steps to ensure that these materials are not available to unauthorized persons.

Downloading Critical or Confidential Data Approval - Critical or confidential Axio data should not be downloaded from a multiuser system to a personal computer or a workstation unless a clear business need exists and advance permission from the Information Technology Department has been obtained.

Mobile Computer Alternatives - When away from Axio's offices, mobile computer users use either encryption software to protect the critical or confidential data when it is held in internal computer system storage or employ some technique to physically secure removable media on which the critical or confidential data resides.

Record Destruction Schedule - Workers are aware not to destroy Axio's records unless these records appear on a list of records authorized for destruction or can be destroyed according to instructions appearing in Axio's records retention policies.

Critical or Confidential Data Retention for Destruction - Workers do not discard critical or confidential data in publicly accessible trash containers. Rather, they securely retain critical or confidential data until it can be shredded or destroyed with other approved methods.

Portable Computer Backups - Workers who use portable computers make backups of all critical or confidential data resident on these computers prior to taking out-of-town trips. These backups are stored somewhere other than the portable computer's carrying case.

Teleworking

(See Remote Access Policy)

Telecommuting Equipment - Employees working on Axio's business at alternative work sites use Axio-approved computer and network equipment, unless other equipment has been approved by the COO as compatible with Axio's information systems and controls.

Telecommuter and Remote Workers Information Security Procedures - Telecommuters follow all remote system security policies and procedures including, but not limited to, compliance with software license

agreements, performance of regular backups, ensuring that OS security patches and AV software and scanning remains current, and use of shredders to dispose of critical or confidential paper-resident data.

Remote workers connect to the Axio network infrastructure only via secure, encrypted connections to ensure that all data in transit remains encrypted. As noted above, public networks (e.g., libraries, airports, Starbucks) are not to be trusted.

Clean Desk, Clean Screen

Axio employees must always remain cognizant of their surroundings even when working from home or the office. A coworker, relative, or stranger should not be allowed to shoulder-surf, nor should you engage in conversation while you have critical or confidential customer data on your screen. Although we discourage any printing of client information, should you retain physical copies, data must always be kept under lock and key when not being actively used.

Before traveling, this P&P and the Mobile Device Management Security P&P should be reviewed. Special precaution must be taken to prevent bystanders from viewing your screen. Hardcopies of critical or confidential data must not be taken out of the office. Client data should never be viewed by you unless you are at a safe distance where shoulder-surfing (and recording of your screen) isn't possible. [KC24.5]

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27002:2013 – 6 Organization of Information Security
ISO/IEC 27002:2013 - 8.1.3 Acceptable Use of Assets
ISO/IEC 27002:2013 – 9.3 User Responsibilities
ISO/IEC 27002:2013 – 12 Operations Security
AT 101 – SOC 2: CC1.0 – Common Criteria Related to Organization and Management
AT 101 – SOC 2: CC2.0 Common Criteria Related to Communications
AT 101 - SOC 2: CC5.0 - Common Criteria related to Logical and Physical Access Controls
AT 101 - SOC 2: CC7.0 - Common Criteria Related to Change Management
AT 101 – SOC 2 – C1.1 to C1.6 – Additional Criteria for Confidentiality
HIPAA Security Rule 164.316(a) – Policies and Procedures

Axio Encryption Standard, Policy, and Procedures

Purpose:	This document details Axio's standard regarding the use of encryption to protect Axio's critical and confidential data. All protection of data must abide by regulatory standards as well as all internal policies, standards, and procedures that Axio establishes. [KC25.1]
Applies To:	This standard applies to all data that is defined as critical or confidential per the Data Classification policy. Critical and confidential data is to be protected during transit and at rest.
Last Updated:	August 21, 2019

Responsibilities

Users: All users are responsible for knowing and putting into practice the Axio standard on encryption requirements to protect Axio's information assets.

Information Technology:

- Ensures all encryption requirements are enforced on Axio's endpoints
- Ensures all encryption requirements are enforced during transportation
- Ensures all internal portals and websites are encrypted with current SSL/TLS standards, while ensuring deprecated ciphers and standards are prevented

Standard Requirements

- Internal organizational systems use strong, industry acceptable encryption algorithms.
- Internal organizational systems prevent renegotiation of weaker encryption standards.
- Encryption methods are used for internal communications whenever possible through the use of VPN, SSH, SSL/TLS, or IPSEC, especially when dealing with critical or confidential data. [KC25.2]
- Whenever wireless communications are used, they maintain the minimum of WPA2 Enterprise encryption.

Policy Statements

Digital Certificate Revocation

In the event an employee laptop or other device is lost or taken out of service, the digital certificates associated with that piece of equipment is placed on the respective Certificate Authority's certificate revocation list (CRL).

Encryption Rules

Encryption is used according to the following rules:

- All customer data would be encrypted in storage, as well. At present, no critical customer systems are hosted locally.
- All external connections to Axio data are through secure, encrypted connections such as VPN. [KC25.2]
- All laptops have full disk encryption placed on them to prevent loss of information if theft occurs.
- All communications to customers, clients, and third parties that contain customer account data or other critical or confidential data is encrypted.

Encryption Mechanisms

The following encryption mechanism standards are used:

- Digital certificates are only obtained from trusted Certificate Authorities and are in place to encrypt traffic on all public-facing application servers.
- Encryption keys will be rotated as frequently as Axio determines acceptable based on risk related to information loss. [KC25.3]
- If keys are compromised or suspected of compromise, they will be rotated immediately.
- Stored keys are stored only encrypted and unreadable. Axio uses Google Key Management.
- All passwords or passphrases for users, databases, information systems, and devices inside the company are stored in encrypted form.
- Key custodian personnel have been restricted to the minimum number of personnel who need to have access to the system.
- Axio requires the use of AES-256-bit encryption strength and a SHA-2 hashing algorithm for symmetric-key algorithms, which are the current secure encryption protocols. Asymmetric-key algorithms are in place when public-key encryption and digital signatures are required for secure communications (e.g., TLS on Axio's payment portals).
- In the Axio environment, the following encryption tools are in place:

Area	Products in use at Axio
Email Encryption	Not Applicable
File Encryption	Box
Full Disk Encryption	FileVault2 on end-user devices
File Transfer Encryption	HTTPS for any customer file uploads
Wireless Networking	WPA2

Secure File Sharing Procedures

Sharing Via Email

1. Save the document as a pdf. Open the pdf in Preview. (If you are sending a PowerPoint document, start by using the Export command in PowerPoint to create the initial pdf instead of the Print command.)
2. Select the File - Export as pdf… command.
3. Click on Show Details.
4. Click on the Encrypt check box.
5. Set a strong password and record the password in the customer-specific vault in 1Password.
6. Convey the password to the customer in an alternate channel to the delivery of the document.

Sharing Via Box

If you need to collaborate with customers on an ongoing basis, the Axio box.com enterprise license supports essentially unlimited external collaborators. If you need to share, create a folder, clearly label it as “external shared” so you don’t accidentally put internal files in the folder, and share the folder using the external person’s email address (rather than giving them an anonymous link to the folder).

Exemptions

Exemptions to this policy must be approved in accordance with the Risk Management policy. A policy exemption does not release users from their responsibility to protect Axio’s information resources.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Axio reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Axio does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Axio reserves the right not to defend or pay any damages awarded against employees or partners which result from violation of this policy.

Any employee or partner who is requested to undertake an activity which he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager, any other manager, or the Human Resources Department as soon as possible.

References

ISO/IEC 27001 – A.9.4 System & Application Access Control
ISO/IEC 27001 – A.10 Cryptography
ISO/IEC 27001 – A.18.1.5 Regulation of Cryptographic Controls
AT 101 – SOC 2: CC6.0 - Common Criteria Related to System Operations

Appendix A: Key Control Objectives

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
1.1	Annual Acknowledgement of Information Security Policies by employees and contractors	CC1.1	CC1.4	CC2.2	CC2.3					
1.2	Annual Review of Information Security Policies by Management	CC1.4	CC1.5	CC5.3	CC3.1	CC2.1				
1.3	Policy & Procedures identify the key controls and provide basic guidelines for employees to execute critical tasks.	CC1.5	CC6.1	CC5.3	CC3.1	CC2.1				
1.4	Notice of Disciplinary Action for Information Security policy violations	CC1.1								
1.5	Accountability for Key Controls	CC1.5	CC5.3	CC3.1	CC2.1					
1.6	Management Identifies Confidential Data and Assigns Owners *to the Data, as well as, Systems* that House, Access and Process Confidential data.	CC1.5	CC8.1							
1.7	Axio Maintains up-to-date Organizational Charts with review/revision date	CC1.1	CC1.3	CC3.1						
1.8	Job Descriptions Provided and Updated as needed	CC1.3	CC2.2	CC2.3	CC5.3					
1.9	Policies and Procedures are centrally located for employees to access.	CC2.3	CC5.3	CC2.1						
2.1	Axio conducts an annual Risk Assessment	CC3.2	CC3.3	CC9.1	CC3.4	CC3.1				
2.2	Quarterly Information Security Meetings	CC5.1	CC5.2							
2.3	Monitoring to ensure timely security software patch updates and Identified Security Vulnerabilities Investigated in a Timely Manner.	CC5.1	CC5.2	CC8.1						
2.4	Auditing of Unauthorized Access Attempts into Production Environment	CC4.1	CC4.2	CC5.1	CC5.2	CC7.2				
2.5	Infrastructure Health Monitored and Investigated in a Timely Manner	CC4.1	CC4.2	CC5.1	CC5.2	A1.1				
2.6	Annual Audit of Security, Availability and Confidentiality Controls	CC3.2	CC3.3	CC3.1						

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
2.7	Analysis of Testing Results section of Significant Vendor Annual Independent Audit Reports	CC5.1	CC5.2	CC6.4	CC6.5	CC9.2	CC3.4			
2.8	Axio has a vulnerability scans done semiannually, and penetration test conducted annually.	CC5.1	CC5.2							
2.9	Axio has contracts with their customers communicates their commitments and the associated system requirements. Information regarding the design and operation of the system and its boundaries has been prepared and communicated to permit users to understand their role in the system and the results of system operation. Customers have been provided with information on how to report failures, incidents, concerns, and other complaints to appropriate personnel.	CC2.2	CC2.3							
2.10	Executive management met annually with operational management to assess the effectiveness and performance of internal controls within the environment.	CC1.2								
3.1	Pre-employment background checks	CC1.1								
3.2	Acknowledgment of Employee Handbook and/or code of conduct, Confidentiality Agreement and Information Security Policy upon Hiring	CC1.1								
3.3	Signed Non-Disclosure Agreements for Third Parties	CC2.2	CC2.3							
3.4	Timely Notification and Removal of physical and logical access	CC4.1	CC4.2	CC6.3						
3.5	Axio employees including executives receive annual reviews from their supervisor.	CC1.1	CC1.4	CC3.1						
3.6	Checklist (termination procedures) completed for terminated employees	CC1.1	CC6.2							
3.7	Management completes an onboarding checklist (hiring procedures) for new hires	CC1.1								
3.8	New hire resume showing the new hire has competency or skills and experience and it was verified.	CC1.4								
3.9	Employees are required to attend continued training annually that related to their job role and responsibilities.	CC1.4								

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
4.1	Contract Language supports Effective Oversight Measures and Control over Third-Party Contractors	CC2.2	CC2.3	CC9.2						
4.2	Management annual review of risk, contract terms and granting of third-party access	CC2.2	CC2.3	CC9.2	CC1.3					
4.3	Access & Permissions Authorization based on User	CC2.2	CC2.3							
4.4	Third-Parties who are granted Infrastructure Access require Acknowledgement of InfoSec, Acceptable-Use and Confidentiality policies and procedures	CC2.2	CC2.3	CC9.2						
4.5	Third-Parties who are granted Infrastructure Access must sign NDA	CC2.2	CC2.3	CC9.2						
5.1	Annual Security Awareness Training of employee-base reinforces confidential data guideline	CC1.4	CC2.2	CC2.3	CC2.3					
5.2	Confidential Data access authorized by the functional Department Manager as well as the Data/System owners.	CC2.3	CC6.1	CC6.2	CC8.1					
5.3	Use of Privileged IDs challenged during Semi Annual Access Reviews	CC4.1	CC4.2	CC6.1	CC6.3					
5.4	User passwords, including Privileged User ID passwords, are encrypted during transmission and at rest.	CC6.6	CC6.7							
5.5	Customer PII encrypted at rest	CC6.6	CC6.7							
5.6	Axio employees only connect to production environments through encrypted channels	CC6.3	CC6.7							
6.1	Periodic Reassessment of Data Locations and Classifications	C1.1								
6.2	Confidential data cannot be recovered once destroyed.	CC6.1	C1.2							
7.1	Infrastructure Inventory Maintained	CC6.1	C1.1							
7.2	Employee & Contractor Equipment must meet Axio hardening guidelines for end-user equipment	CC6.1								
8.1	IT Department ensures proper information disposal with qualified 3rd-party vendors, when needed	CC6.7	C1.2							
9.1	Badge Controlled Access to Offices	CC6.4	CC6.5							
9.2	Facility visitor log maintained	CC6.4	CC6.5							
9.3	Physical Access to Facilities Revoked in a Timely Manner	CC4.1	CC4.2	CC6.4	CC6.5					

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
9.4	Axio obtains and analyzes annual, 3rd-Party infrastructure support providers, independent audit reports for exceptions.	CC6.4	CC6.5	CC9.2						
9.5	Maintenance records are retained when repairs/changes must be made to physical and environmental safeguards (e.g. fire suppression inspection; replace badge systems, UPS testing, etc.)	CC6.4	CC6.5							
9.6	Employees Are Responsible for the Physical Security of Mobile Devices	CC6.4	CC6.5							
9.7	Review of Badge Access system to badges issued	CC4.1	CC4.2							
10.1	Access & Permissions Authorization based on Principle of Least-Privilege	CC6.1								
10.2	Privileged User Account Access Limited to Authorized Users	CC2.2	CC2.3							
10.3	Write-access to the Production Database is Strictly Limited	CC8.1								
11.1	All Employees, Contractors & Customers are Assigned Unique IDs	CC6.1	CC6.2							
11.2	Customer IDs and password combinations are authenticated within AWS Cognito for the SaaS offering.	CC6.1								
11.3	Administrator and other Privileged User IDs are Restricted to Authorized Personnel	CC6.1								
11.4	Validation of User Identity prior to Revising Authentication Credential	CC6.1	CC6.2							
11..5	Authorization of user privileges by functional Department Manager and system/data owner (Confidential Data/System)	CC6.1	CC6.2							
11.6	Axio application captures logging of user access and activity	CC4.1	CC4.2							
11.7	Semi-annual Access Reviews of Critical Infrastructure Systems	CC4.1	CC4.2	CC6.3						
11.8	Workstations are Configured to Lock after 15 minutes of Inactivity	CC6.1	CC6.2							
12.1	Complex Passwords required to access all critical systems	CC6.1								
12.2	Passwords are encrypted at rest in Database and in Transit	CC6.6	CC6.7							
12.3	Account Lockout after 6 Failed Access Attempts	CC6.1	CC6.2							

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
12.4	Application passwords are Encrypted and Access to Them Is Restricted to Authorized Personnel	CC6.1	CC6.7							
13.1	Production Servers Hardened via Access Control Lists, and Port and Services Restrictions	CC6.1								
13.2	Axio monitors its infrastructure for outdated software and antivirus patches	CC6.8	CC8.1	-	-	-	-	-	-	-
13.3	Axio applies the "default deny" principle and security hardening techniques to all Production servers/instances.	CC6.6								
13.4	Network Diagram maintained for infrastructure configuration monitoring	CC6.6								
13.5	Wireless access points are hardened, access to the internal network is segregated and require additional authentication	CC6.1								
13.6	Encryption of User Credentials Upon Transmission	CC6.7								
13.7	Network Saturation, CPU loads and Device Memory Monitoring	CC7.2	A1.1							
13.8	Network scans looking for vulnerabilities in the infrastructure	CC6.6								
14.1	Authorization of Access to Network/Firewall by CIO or his designee	CC6.6								
14.2	Firewall Hardened to least connectivity required for application	CC6.1	CC6.6							
14.3	Default Deny Principle Applied to Infrastructure Resources	CC6.6								
14.4	Firewall Logging of Failed Login Attempts	CC4.1	CC4.2	CC6.6	CC7.2					
14.5	Timely Firewall Patching	CC8.1								
14.6	Specific Protocol Required to Initiate and Support Firewall Change	CC6.6								
14.7	Firewall Configuration Files managed by GCP	CC6.6								
14.8	Core Production Network Configurations are Reviewed every 6 Months	CC6.6								
15.1	Remote Access Transmissions Into Infrastructure Equipment Require Strong Encryption and Multi-Factor	CC6.2	CC6.3							

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
15.2	Complex passwords required (per Information Access Management Policy) to gain remote access to Corporate Network via VPN	CC6.1	CC6.2							
15.3	Timely patching of Infrastructure Equipment	CC8.1								
15.4	Timely Revocation of Remote and Network Access if user is terminated or user equipment is lost or compromised.	CC4.1	CC4.2	CC6.2						
16.1	Antivirus Installed across all Axio Critical Infrastructure	CC6.8								
16.2	Antivirus patches auto-updated, wherever possible, and monitored across all Axio critical infrastructure	CC6.8								
16.3	Antivirus Scans across the infrastructure are Automated to Run Periodically	CC6.8								
16.4	Antivirus Scanning of Downloaded Files	CC6.8								
17.1	Logging and alerting on system health issues and intrusion detection	CC4.1	CC4.2	A1.1						
17.2	Timely Log Monitoring	CC4.1	CC4.2							
17.3	Axio application captures logging of user access and activity	CC4.1	CC4.2							
17.4	User Logging & Monitoring on Network, Firewall and Production Servers	CC4.1	CC4.2	CC6.1						
18.1	Back-up of code and database files to off-site servers, nightly	CC7.2	A1.2	A1.3						
18.2	Back-up Failure Alerts are Received and Resolved in a Timely Manner	CC7.2	A1.2	A1.3						
18.3	Restores of database backups are performed, as needed, but at least annually.	CC4.1	CC4.2	A1.2	A1.3					
18.4	Backups are retained for 90 days	CC7.2	A1.2							
18.5	Backups are encrypted in transit and at rest	CC6.7								
18.6	Axio has a Business Continuity Plan with revision history	CC5.1	CC5.2	CC6.1	CC6.4	CC6.5	CC6.7	A1.3		
18.7	Contract in place with the offsite backup storage vendor and the most recent backup rotation log (if applicable)	CC6.7	A1.3							
19.1	Configuration files backed up by backup tool and by change owner prior to requesting infrastructure change to support roll-back	CC8.1								

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
19.2	Axio Assigned Individual(s) Responsible for Monitoring and Maintaining the Customer Application and Data Infrastructure	CC8.1	CC2.1							
19.3	Requirements and Acceptance Criteria to Meet Are Defined, when applicable	CC8.1								
19.4	There is evidence of review and approval of All Infrastructure Changes	CC8.1								
19.5	Infrastructure inventory/diagram updated (as needed)	CC3.2	CC3.3	CC8.1	CC2.1					
19.6	Proposed infrastructure changes impacting customer services availability communicated in writing to customers	CC8.1								
19.7	Testing/QA performed to ensure hardening guideline are met	CC8.1								
19.8	Proposed infrastructure changes impacting employees are communicated in writing.	CC8.1								
19.9	Tickets produced for all infrastructure changes and patches	CC8.1								
20.1	Axio has written code change management procedures to be followed by Development.	CC8.1								
20.2	Requirements and Testing to Meet are Defined	CC8.1								
20.3	Authorization of Code Change	CC8.1								
20.4	Code Review & Unit Testing (and Regression where applicable) Performed by Independent Developer/QA	CC8.1								
20.5	Change Tested in a Dev Environment to Ensure No System Degradation	CC8.1								
20.6	UAT Validate that the Business Requirements and Functional Testing Were Met	CC8.1								
20.7	Code Vulnerability Scanning Performed (remove if they don't have)	CC8.1								
20.8	Developers do Not Have Write-access to Production Databases.	CC8.1								
20.9	Confidential Data is Not Stored in Dev Environment.	CC8.1								
20.10	Tickets produced for all application changes	CC7.3	CC7.4	CC7.5						
21.1	Encryption of Sensitive Data	CC6.1	CC6.6	CC6.7						

Ctrl #	Key Control Objectives per Policies	2017 Trust Services Criteria								
21.2	Email users are authenticated by Okta	CC6.7								
22.1	Mobile Device Guidelines Established	CC2.3	CC6.6							
22.2	Users Are Responsible for Maintaining Up to Date OS and AV Patches on Their Devices	CC2.3	CC8.1							
22.3	Laptop Encryption and Remote Data Wiping on Laptops is Enabled	CC6.7								
22.4	Preapproval and Encryption Required for Media Removal	CC6.7								
23.1	Annual Risk Assessment focusing on risks specific to IT and fraud/illegal acts	CC3.2	CC3.3	CC7.2	CC7.1					
23.2	All employees and contractors must acknowledge understanding and adherence to the Incident Management Policy	CC2.2	CC2.3	CC7.2	CC7.1					
23.3	Intrusion Prevention-Detection Monitoring as well as Monitoring of Unauthorized Access Attempts Generate Alerts	CC2.2	CC2.3	CC4.1	CC4.2	CC7.2	CC7.1			
23.4	Security Incidents are Documented, Tracked, Action Taken is noted and then Reviewed to reduce likelihood of similar exploits.	CC2.2	CC2.3	CC4.1	CC4.2	CC7.2	CC7.1			
23.5	Security Incidents requiring System Downtime and/or Significant System Changes are Communicated to Customers in a Timely Manner	CC2.2	CC2.3	CC3.2	CC3.3	CC4.1	CC4.2	CC 7.3	CC 7.4	CC7. 5
24.1	Annual Acknowledgement to Acceptable-Use of company assets	CC2.2	CC2.3	CC6.1						
24.2	Axio ensures that all employees and contractors are assigned unique user IDs	CC6.2								
24.3	Computer and/or Password Sharing Is Strictly Prohibited	CC6.1								
24.4	Supervisory Approval Must Be Obtained Prior to Any Software Implementation	CC6.3	CC8.1							
24.5	Clean Desk-Clean Screen	CC6.1								
25.1	Cryptographic controls contingent on regulatory & organization's risk assessment	CC6.1	CC6.6	CC6.7						
25.2	Use strong cryptography and security protocols	CC6.1	CC6.6	CC6.7						
25.3	Cryptography key lifecycle use, protection and management	CC6.1	CC6.6	CC6.7						

Appendix B: Revision History

Date	Version	Created By	Approved By	Description of Change
7/23/2019	1.0	Audit Liaison	Dan Hirt	Policy Creation
8/28/2019	1.1-1.2	Pamela Curtis, Lisa Young, Craig Shuster	Lisa Young	Edited, reformatted, and added content from existing Axio Security and Privacy Policy
9/26/2019	1.3	Pamela Curtis	Lisa Young	Final edits based on feedback from reviews
1/3/2020	1.4	Pamela Curtis		Added sections on reporting phishing attempts (in email security section), secure file sharing procedures (in encryption section), and turning off Bluetooth on mobile devices when traveling (in mobile devices section).