EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Education Law §2-d Bill of Rights for Data Privacy and Security for Canton Central School District

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.
3. This right may not apply to parents of an Eligible Student.State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights

Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacysecurity/report-improper-disclosure by mail to: Tim Archetko, 99 State Street Canton, NY 13617, by email to dpo@ccsdk12.org or by telephone at (315)386-8561
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older. [2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.

[2] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data.

CONTRACTOR	
[Signature]	Melissa Palank Digitally signed by Melissa Palank Date: 2025.06.23 16:50:30 -05'00'
[Printed Name]	Melissa Palank
[Title]	Director, JostensPIX Operations
Date:	06/23/25

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	**Jostens**
Description of the purpose(s) for which Contractor will receive/access PII	**School Photography**
Type of PII that Contractor will receive/access	Check all that apply: X Student PII ☐ APPR Data
Contract Term	Contract Start Date July 1, 2025 Contract End Date June 30, 2026
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) X Contractor will not utilize subcontractors. ☐ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data upon request.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) X Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Information is only accessed by those necessary to perform Contractor obligations.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	Melissa Palank Digitally signed by Melissa Palank Date: 2025.06.23 16:51:19 -05'00'
[Printed Name]	Melissa Palank
[Title]	Director, JostensPIX Operations
Date:	06/23/2025

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See Jostens Cybersecurity Compliance Program
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Jostens Cybersecurity Compliance Program
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Onboarding and annual training include training on privacy/handling of personal information; See Jostens Cybersecurity Compliance Program
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	See Jostens Cybersecurity Compliance Program
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	See Jostens Cybersecurity Compliance Program
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Jostens Cybersecurity Compliance Program
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Jostens Cybersecurity Compliance Program
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	CYBERSECURITY PRACTICES ALIGNMENT: The National Institute of Technology & Standards (NIST) Cybersecurity Framework (NIST CSF) represents leading industry-accepted best practices for cybersecurity. Therefore, Jostens' minimum security requirements are consistent with NIST CSF controls to ensure due care and due diligence in maintaining its cybersecurity program.

9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	See Jostens Cybersecurity Compliance Program
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	See Jostens Cybersecurity Compliance Program
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	See Jostens Cybersecurity Compliance Program
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	See Jostens Cybersecurity Compliance Program
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	See Jostens Cybersecurity Compliance Program
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints,	See Jostens Cybersecurity Compliance Program

Function	Category	Contractor Response
	risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	See Jostens Cybersecurity Compliance Program
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	See Jostens Cybersecurity Compliance Program
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	See Jostens Cybersecurity Compliance Program
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	See Jostens Cybersecurity Compliance Program
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	See Jostens Cybersecurity Compliance Program
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	See Jostens Cybersecurity Compliance Program
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	See Jostens Cybersecurity Compliance Program

Function	Category	Contractor Response
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	See Jostens Cybersecurity Compliance Program
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	See Jostens Cybersecurity Compliance Program
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	See Jostens Cybersecurity Compliance Program
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	See Jostens Cybersecurity Compliance Program
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	See Jostens Cybersecurity Compliance Program
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	See Jostens Cybersecurity Compliance Program
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	See Jostens Cybersecurity Compliance Program
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	See Jostens Cybersecurity Compliance Program
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	See Jostens Cybersecurity Compliance Program
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	See Jostens Cybersecurity Compliance Program

CYBERSECURITY COMPLIANCE PROGRAM

Jostens, Inc.

PUBLIC

Public Release Authorized

Table of Contents

JOSTENS COMPLIANCE PROGRAM OVERVIEW

JOSTENS COMPLIANCE POLICY

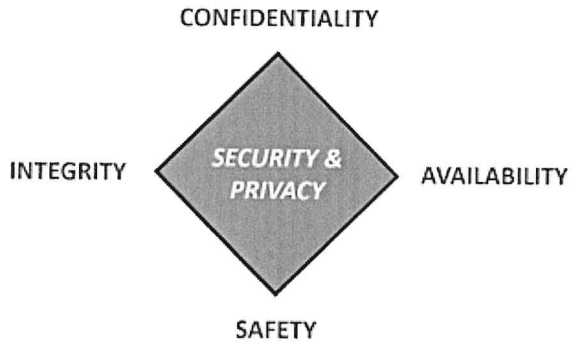
Jostens will protect the confidentiality, integrity, and availability of data and systems, regardless of how the data is created, distributed or stored. Jostens' security controls are tailored accordingly so that controls can be applied commensurate with the risk and sensitivity of the data and system, in accordance with all legal obligations.

MANAGEMENT DIRECTION FOR CYBERSECURITY

The objective of the Jostens Compliance Program is to provide cybersecurity requirements that are in accordance with Jostens' business requirements, as well as relevant laws and other legal obligations for data security and privacy. [1]

Jostens is committed to protecting its customers, employees, partners, and Jostens from damaging acts that are intentional or unintentional. Protecting Jostens data and the systems that collect, process and maintain this data is of critical importance. Therefore, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensures the confidentiality, availability and integrity of the data:

Commensurate with risk, cybersecurity and privacy measures are implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction. The security of systems includes controls and safeguards to offset possible threats, as well as controls to ensures confidentiality, integrity, availability and safety:



- CONFIDENTIALITY – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- INTEGRITY – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- AVAILABILITY – Availability addresses ensuring timely and reliable access to and use of information.
- SAFETY – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Security measures are taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes against accidental loss or destruction.

SCOPE

The requirements of the compliance program apply to all vendors, contractors, consultants, interns or other third-parties that support Jostens operations. This includes all stakeholders involved in transmitting, processing and storing Jostens data.

CYBERSECURITY PRACTICES ALIGNMENT

The National Institute of Technology & Standards (NIST) Cybersecurity Framework (NIST CSF) represents leading industry-accepted best practices for cybersecurity.[2] Therefore, Jostens' minimum security requirements are consistent with NIST CSF controls to ensure due care and due diligence in maintaining its cybersecurity program.

[1] ISO/IEC 27002:2013 – 5.1
[2] NIST Cybersecurity Framework - https://www.nist.gov/cyberframework

Cybersecurity Responsibilities

Human Resources Security

1. Requirements for Employment: Jostens maintains contractual agreements with employees, contractors, consultants and/or other third-party staff that formally documents their responsibilities for cybersecurity.

2. Roles and Responsibilities: Jostens defines and documents security roles and responsibilities of employees, contractors and third-party users to incorporate Jostens' data protection control requirements, to the extent permitted by applicable law:
    a. All employees, contractors, and third-party users are notified of the consequences for not following your security policy in handling Jostens data.
    b. All assets used to manage or store Jostens data are protected against unauthorized access, disclosure, modification, destruction or interference.
    c. All employees, contractors and third-party users are provided with education and training in privacy and security procedures and the correct information processing requirements.
    d. All personnel with access to sensitive Personally Identifiable Information (sPII) must complete a privacy training class and be knowledgeable of any specific privacy requirements for the data being handled. Refresher training is required at least on an annual basis.

3. Assigned Ownership: Jostens assigns ownership of critical and sensitive information, business applications, computer systems and networks to individuals (e.g., business managers) and document the responsibilities of these assigned owners.
    a. Responsibilities for protecting critical and sensitive information, business applications, computer systems and networks are communicated to and accepted by owners.

4. Personnel Screening: Jostens ensures a secure workforce. Background verification checks on all candidates for employment are carried out in accordance with relevant laws, regulations, and ethics and are proportional to the business requirements and the classification of the information that may be accessed.

5. Staff Agreements: Jostens establishes agreements with employees that specify cybersecurity responsibilities. This agreement is incorporated into the contracts of employees, contractors, consultants and/or other third-party staff and taken into account when screening applicants for employment.

Cybersecurity Education & Awareness

1. Cybersecurity Awareness: Jostens employees, contractors, consultants and/or other third-party staff are made aware of the key elements of cybersecurity, why it is needed, and understand their personal cybersecurity responsibilities. A security awareness program is undertaken to promote security awareness to all individuals who have access to the information and systems of the enterprise.

2. Cybersecurity Education: Jostens employees, contractors, consultants and/or other third-party staff are trained in how to run systems correctly, as well as how to develop and apply security controls.

Information Risk Analysis

1. Risk Analysis: Jostens performs information risk assessments of critical areas of its business to identify key information risks and determine the controls required to keep those risks within acceptable limits.
    a. Assessments must include, but are not limited to:
        i. Business environments;
        ii. Business processes;
        iii. Business applications (including those under development);
        iv. Computer systems, and
        v. Networks.

Asset Management

1. Classification: Jostens utilizes a cybersecurity classification scheme that applies throughout the enterprise.

2. Asset Management: Jostens manages essential information about hardware, software, and data flows/extracts/interfaces (e.g., unique identifiers, version numbers, data recipients, physical locations) in inventory:
    a. An appropriate set of procedures for labeling and handling has been developed and implemented.
    b. Personal use of Jostens equipment and data is not allowed.

3. Handling Information: Jostens ensures additional protection is provided for handling sensitive material or transferring sensitive information.
    a. Files containing personal information or business sensitive information are transferred (e.g., email, faxes, etc.) via secure/encrypted file transfer protocols;
    b. Sensitive information is encrypted on all devices, including portable devices, such as laptops, portable media (flash drives) and data backups; and
    c. Jostens' minimum encryption requirement is 128-bit AES.

4. Supply Chain: Jostens ensures that reliable and approved hardware and software are acquired that follows consideration of security requirements. Vigilance are maintained to prevent counterfeit hardware and software from being used anywhere in the enterprise.

Identity and Access Management

1. Access Control: Jostens restricts access to the application and associated information to authorized individuals. This are enforced accordingly to ensures that only authorized individuals to gain access to business applications, systems, networks and computing devices, that individual accountability is assured and to provide authorized users with access privileges that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

2. User Authorization: Jostens ensures that all users have authorization before they are granted access privileges.
    a. User access privileges are reviewed at least every six (6) months; and
    b. Access are revoked immediately upon change in role or employment status.

3. User Authentication: Jostens ensures strong user authentication is implemented throughout the enterprise:
    a. All users are authenticated by an individual identifier, not group or shared identifiers; and
    b. Strong authentication mechanisms are used in conjunction with the identifier (e.g., strong passwords, smart cards or biometric devices) before the user can gain access to systems or data.

4. Privileged Accounts: Jostens ensures that accounts with privileged access are separate from a user's normal, non-privileged account.

5. Off-Premise Access Control: Whenever technically feasible, Jostens ensures cloud solutions offer the option to be federated to Jostens systems for authentication using Jostens credentials.

Physical and Environmental Security

1. Facilities: Jostens secures facilities where Jostens data is stored, processed or transmitted:
    a. The number of entrances to the information processing facilities in which Jostens data is stored are limited.
        i. Every entrance into these areas requires screening. (e.g., security guard, badge reader, electronic lock, a monitored closed caption television (CCTV)).
        ii. Access logs are recorded and maintained.
    b. Physical access is restricted to those with a business need.
        i. Access lists are reviewed and updated at least once per quarter.
    c. Process, training, and policies are in place to determine visitor access, after-hours access, and prevent tailgating into controlled areas.
    d. Emergency exits in controlled areas must sound an alarm when opened and include automatic closure.
        i. Any alarms must trigger an emergency response.

2. Physical Protection: Jostens actively manages the physical security controls and ensures all buildings throughout the enterprise that house critical IT functions (e.g., data centers, network facilities, and key user areas) are physically protected from unauthorized access.

3. Hazard Protection: Jostens ensures computer equipment and facilities are protected against natural and man-made hazards.

4. Power Supplies: Jostens protects critical computer equipment and facilities against power outages.

System Configuration

1. Host System Configuration: Jostens configures host systems according to an industry standard.
    a. Systems are configured to function as required and to prevent unauthorized actions.
    b. Examples of best practice configuration include, but are not limited to:
        i. Center for Internet Security (CIS)
        ii. US Department of Defense Secure Technical Implementation Guides (STIGs)
        iii. OEM best practices (e.g., Microsoft, VMware, Oracle, etc.)

2. Mobile Devices: Jostens maintains policies, standards, and procedures covering the use of mobile/portable devices.
    a. The use of mobile devices (e.g., smartphone, iPad, tablet, USB memory sticks, external hard disk drives, MP3 players, e-book readers, etc.) are:
        i. Subject to approval; and
        ii. Access is restricted.
    b. Controls are implemented to ensures that sensitive information stored on these devices is protected from unauthorized disclosure.

System Monitoring

1. Event Logging: Jostens logs all key cybersecurity events, including but not limited to:
    a. All actions taken by any individual with root or administrative privileges;
    b. Access to all audit trails;
    c. Invalid logical access attempts;
    d. All individual user accesses to cardholder data;
    e. Use of and changes to identification and authentication mechanisms, including but not limited to:
    f. Creation of new privileged accounts and elevation of privileges; and
    g. All changes, additions, or deletions to accounts with root or administrative privileges;
    h. Initialization, stopping, or pausing of the audit logs; and
    i. Creation and deletion of system-level objects.

2. System Network Monitoring: Jostens implements a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes:
    a. Reviewing the following, at least daily:
    b. All security events;
    c. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
    d. Logs of all critical system components; and
    e. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
        i. Firewalls;
        ii. Intrusion Detection Systems (IDS);
        iii. Intrusion Prevention Systems (IPS); and
        iv. Authentication servers (e.g., Active Directory domain controllers); and
    f. Following up exceptions and anomalies identified during the review process.

3. Intrusion Detection / Prevention: Jostens implements and monitors Intrusion Detection System (IDS) mechanisms on all critical systems and networks.

Network Security

1. Defense In Depth (DiD): Jostens secures its computer networks using multiple layers of access controls to protect against unauthorized access. In particular:
    a. Group network servers, applications, data, and users into security domains;
    b. Establish appropriate access requirements within and between each security domain; and
    c. Implement appropriate technological controls to meet those access requirements consistently, including (for example) firewalls.

2. Network Controls: Jostens ensures that all data and communications networks are secured to ensures the transmission of data is kept confidential.
    a. Applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for business functionality, are disabled or removed;
    b. Network segments connected to the Internet are protected by a firewall which is configured to secure all devices behind it;
    c. Network segments where Jostens data resides are isolated from non-Jostens data, logically or physically unless approved by Jostens Security;
    d. User connection capability are documented with regard to messaging, electronic mail, file transfer, interactive access, and application access;
    e. All production servers are located in a secure, access-controlled location;
    f. Firewalls are configured properly to address all reasonably-known security concerns;
    g. Infrastructure diagrams, documentation, and configurations are up to date, controlled and available to assist in issue resolution; and
    h. Systems must have the ability to detect a potential hostile attack. (e.g., IDS/IPS)
        i. All systems are updated to the current release and actively monitored.

3. Wireless Access: Wireless access are authorized, authenticated, encrypted and permitted only from approved locations.

4. Remote Access: Remote access to a network containing Jostens data are done via a secure connection (e.g., VPN).
    a. All extranet connectivity into Jostens are through Jostens-approved and authorized secure remote connections.

Cryptography

1. Cryptography: Jostens cryptographic solutions must:
    a. Meet or exceed Jostens' minimum encryption requirement of 128-bit AES; and
    b. Protect the confidentiality of sensitive information that is subject to legal and regulatory-related encryption requirements.

2. Cryptographic Key Management: Jostens manages cryptographic keys, in accordance with industry-recognized leading practices for key management:
    a. Documented standards and procedures must exist; and
    b. Cryptographic keys are protected against unauthorized access or destruction to ensures that these keys are not compromised (e.g., through loss, corruption or disclosure).

Information Privacy

1. Information Privacy: Jostens establishes responsibilities for managing information privacy and data security controls for handling sensitive Personally Identifiable Information (sPII).

2. Alignment with Jostens Privacy: Jostens ensures sPII is collected, used, stored, transferred, and destroyed according to Jostens' privacy requirements.

Malware Protection

1. Malware Controls: Jostens implements and manages enterprise-wide detection, prevention and recovery controls to protect against malware that includes having procedures and assigned responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks.

2. Malware Prevention: Jostens ensures the installation and regular update of malware detection and repair software to scan systems and media as a precautionary control, or on a routine basis. The scan carried out should include:
    a. Scan any files received over networks or via any form of storage medium, for malware before use;
    b. Scan electronic mail attachments and downloads for malware before use; and
    c. Scan web pages for malware.

Vulnerability Management

1. Vulnerability Management: Jostens ensures a vulnerability management program exists to eliminate vulnerabilities that could be exploited by malware or other technical methods (e.g., exploitation through technical vulnerabilities). This includes, but is not limited to:
    a. Vulnerability remediation;
    b. Software and firmware patching; and
    c. Hardware maintenance.

2. Web-Enabled Applications: Jostens implements and manages specialized technical controls for web-enabled applications to ensures that the increased risks associated with web-enabled applications are minimized:
    a. All internets facing websites are scanned for security vulnerabilities that potentially open the site up to malicious behavior.
    b. Jostens' minimum list of validation is the Open Web Application Security Project (OWASP) Top 10 vulnerabilities (e.g., cross-site scripting (XSS), SQL injection, Admin access, open directories, insecure data transfer, etc.).

Communications & Operations Management

1. Communications Security: Jostens supports standards and procedures that ensures confidentiality, integrity, and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.

2. Operations Management: Jostens maintains overall operational control and visibility into all security aspects of how data is processed, stored and transmitted:
    a. System administrators must have adequate training and experience to securely administer the infrastructure within their responsibility;
    b. Jostens have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process; and
    c. Vendors are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.

System Acquisition, Development & Maintenance

1. Specification of Requirements: Jostens takes into consideration the cybersecurity requirements for the system under development when designing the system to ensures Jostens' business requirements (including those for cybersecurity) are documented and agreed upon before detailed design commences.

2. Quality Assurance: Jostens ensures quality assurance activities are performed for critical security controls during the development lifecycle.

3. Testing: Jostens ensures that all elements of a system (e.g., application software packages, system software, hardware, and services) are rigorously tested before the system is promoted to a production environment.

4. Test Data: Jostens ensures any sensitive Jostens business information copied from the production environment are protected by:
    a. Depersonalizing sensitive business information;
    b. Restricting access to business information in the development environment; and
    c. Erasing copies of Jostens business information once testing is complete.

5. Development Methodologies and Environment: Jostens development activities are:
    a. Carried out in accordance with a documented system development methodology;
    b. Performed in specialized development environments;
    c. Isolated from production environments; and
    d. Protected against disruption and disclosure of information.

6. System Design / Build: Jostens ensures system build activities are:
    a. Carried out in accordance with industry-recognized leading practices (e.g., OWASP);
    b. Performed by individuals provided with adequate skills/tools; and
    c. Inspected to identify unauthorized modifications or changes which may compromise security controls.

7. Installation Process: Jostens ensures that newly-promoted systems to the production environment are installed in accordance with the Jostens documented installation process.

8. Post-implementation Review: Jostens ensures a post-implementation review is conducted for all newly-promoted systems to the production environment.

9. Secure Destruction: Jostens ensures methods of destruction are formally implemented, based on the type of media:
    a. Physical, paper-based media;
    b. Physical, digital media; and
    c. Electronic, digital data.

10. Lifecycle Management: Jostens defines the End of Life (EOL) process for all systems and applications which could include date of EOL and any business triggers that may result in updated EOL date;

Change Management

1. Change Control: Jostens documents and manages operating procedures for its change control process(es).

2. Change Management: Jostens ensures that changes to any systems, applications or networks, including "emergency" changes, are reviewed, tested, approved and applied using a change management process.

3. Change Documentation Retention: Jostens ensures that documentation of changes is retained for at least three hundred and sixty-five (365) days.

Cybersecurity Incident Management

1. Incident Management: Jostens documents all cybersecurity incidents and maintain a documented cybersecurity event management process that covers the incident response, escalation, and remediation of Cybersecurity events and incidents.

2. Forensic Investigations: Jostens has an established process for managing incidents that require forensic investigation.

Disaster Recovery

1. Disaster Recovery: Jostens develops, supports and routinely tests Disaster Recovery (DR) activities that address all reasonably-foreseen contingency arrangements.

2. Resilience: Jostens applications, systems, and networks are run on robust, reliable hardware and software, supported by alternative hardware or duplicate facilities.

3. Data Backups: Jostens ensures that backups of essential information and software are performed on a regular basis, according to a defined cycle discussed with and approved by Jostens.

Processing Facilities

1. Comingling of Data: Jostens ensures that when Jostens business information is co-located with non-Jostens data, (e.g., virtual servers, cloud solutions, etc.) the non-Jostens data must at least be logically separated from Jostens business information.

2. Virtualization & Cloud Solutions: Jostens may utilize a cloud solution, which must adhere to the same security principles required by Jostens IT security policies and applicable government regulations, laws, or directives as used throughout the enterprise:
    a. The geographic location of provider infrastructure resources is known to Jostens. Jostens is in control of the data location to ensure compliance with local laws that restrict the cross-border flow of data.
    b. Vendors providing cloud services must:
        i. Provide a process for data destruction and secure deletion of any and all Jostens data as needed;
        ii. Have an established method of encrypting sensitive data in storage and in transit following industry-recognized leading practices;
        iii. Securely handle Jostens related data, compute resources, virtual machines resources by providing logical isolation and secure migration;
        iv. Include methods or options for multi-factor authentication for cloud administrator roles;
        v. Provide Jostens the capability to fully audit Jostens user access and activity within the cloud service. Audit logs are capable of being exported from the cloud service;
        vi. Limit employee access to the least privilege needed to perform their duties.
        vii. Maintain documented audits or established compliance roadmaps in alignment with Industry Standard Certifications for Cloud Security. Examples include ISO27001/2, SSAE16, FEDRAMP, CSA STAR, FIPS 140-2, and Open Data Alliance;
        viii. Demonstrate adherence to Security Development best practices for all code, APIs, and applications deployed and implemented in support of the cloud service;
        ix. Process and advise Jostens of any security breach involving Jostens data or services utilized by Jostens; and
        x. Provide Jostens with the means to monitor in near real-time service and resource availability; and
    c. All access to cloud computing sites must encrypt data in transit.
        i. Any Jostens data stored in a cloud environment is encrypted so that data cannot be read by other users in a multi-tenant environment.

Vendor Management

1. Outsourcing: Jostens operates a formal process to address due care and due diligence considerations in the selection and management of third-party vendors:
    a. These third-party vendors must sign agreements that specify the security requirements to be met before commencing work on behalf of Jostens that could have an impact on Jostens' business operations with the vendor;
    b. These security requirements must align with the provisions expected of Jostens from vendor; and
    c. All subcontracted activities involving Jostens information are approved and secured by vendor.

2. VENDOR Exit Strategy: Jostens ensures a documented termination of service process is in place that ensures Jostens business data is recoverable if Jostens terminates a service agreement with a third-party vendor.

3. Indemnification: Jostens addresses indemnification considerations with third-party vendors that could have an impact on Jostens' business operations with the vendor.

COMPLIANCE

1. Statutory / Regulatory / Contractual Compliance. Jostens maintains a process to be aware of and be compliant with all applicable statutory, regulatory and contractual compliance requirements. Examples include but are not limited to FERPA, COPPA, CCPA, PCI DSS, HIPAA, and SOX.

2. Compliance Status: Jostens has a process to document non-compliance of any statutory, regulatory or contractual requirement:
    a. Jostens identify and quantify the risks and mitigation plans and documents the business decision for alternate controls or risk acceptance; and
    b. The mitigation plan and business decision are signed off by the Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability.

3. Breach Notification: Jostens maintains a documented breach notification process that meets all applicable legal and contractual requirements.

4. Payment Card Industry Data Security Standard (PCI DSS): Jostens does not store customers' cardholder data; however, Jostens falls within scope of PCI DSS compliance and therefore:
    a. Maintains documented compliance with the most current version of the PCI DSS;
    b. Conducts quarterly network scans by an Approved Scanning Vendor (ASV); and
    c. Obtains a Report of Compliance (ROC) from an annual on-site PCI Data Security Assessment with a Qualified Security Assessor (QSA).

GLOSSARY: ACRONYMS & DEFINITIONS

ACRONYMS

AD. Active Directory
APT. Advanced Persistent Threat
BCP. Business Continuity Plan
CDE. Cardholder Data Environment
CERT. Computer Emergency Response Team
CIRT. Computer Incident Response Team
COOP. Continuity of Operations Plan
CTI. Controlled Technical Information [3]
CUI. Controlled Unclassified Information [4]
DAC. Discretionary Access Control
DISA. Defense Cybersecurity Agency
DLP. Data Loss Prevention
DRP. Disaster Recovery Plan
EAP. Extensible Authentication Protocol
EPHI. Electronic Protected Health Information
FICAM. Federal Identity, Credential, and Access Management
FIM. File Integrity Monitor
GDPR. General Data Protection Regulation
HIPAA. Health Insurance Portability and Accountability Act
IRP. Incident Response Plan
ISMS. Cybersecurity Management System
ISO. International Organization for Standardization
LDAP. Lightweight Directory Authentication Protocol
MAC. Media Access Control
NIST. National Institute of Standards and Technology
PCI DSS. Payment Card Industry Data Security Standard
PDCA. Plan-Do-Check-Act
PIV. Personal Identity Verification
RBAC. Role-Based Access Control
TLS. Transport Layer Security

DEFINITIONS

Jostens recognizes two sources for authoritative definitions:

- Unified Compliance Framework (UCF) Compliance Library[5]
- The National Institute of Standards and Technology (NIST) IR 7298, Revision 2, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define common digital security terms. [6]

Security Requirements and Controls

The term control can be applied to a variety of contexts and can serve multiple purposes. When used in the security context, a security control can be a mechanism (i.e., a safeguard or countermeasure) designed to address protection needs that are specified by a set of security requirements.

- Controls are defined as the power to make decisions about how something is managed or how something is done; the ability to direct the actions of someone or something; an action, method, or law that limits; or a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system.
- Requirements are defined as statements that translate or express a need and its associated constraints and conditions.[7]

[3] CUI Registry - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html
[4] CUI Registry - https://www.archives.gov/cui/registry/category-list
[5] UCF Compliance Library - https://compliancedictionary.com
[6] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
[7] ISO/IEC/IEEE 29148