GAT Labs

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and GAT Labs **("Vendor")** are parties to a contract dated 14/02/2024 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, GAT Labs for Edu ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means GAT Labs.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Signatures

For Wayne-Finger Lakes BOCES/EduTech	For GAT Labs
Date 2/28/24	**Date** 27 February 2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

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. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
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 at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained 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, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech

Date 2/28/24

For GAT Labs

Date 27 February 2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment C – Vendor's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attach)

Information Security Policy

Policy Owner: CEO, DPO

Effective Date: 2023-03-24

Overview

This Information Security Policy is intended to protect General Audit Tool Ltd.'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of General Audit Tool Ltd.. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every General Audit Tool Ltd. employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of General Audit Tool Ltd.'s information and assets. These rules are in place to protect customers, employees, and General Audit Tool Ltd.. Inappropriate use exposes General Audit Tool Ltd. to risks including virus attacks, compromise of network

systems and services, financial and reputational risk, and legal and compliance issues.

The General Audit Tool Ltd. "Information Security Policy" is comprised of this policy and all General Audit Tool Ltd. policies referenced and/or linked within this document.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct General Audit Tool Ltd. business or interact with internal networks and business systems, whether owned or leased by General Audit Tool Ltd., the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at General Audit Tool Ltd. are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with General Audit Tool Ltd. policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at General Audit Tool Ltd., including all personnel affiliated with third parties. This policy applies to all General Audit Tool Ltd. controlled company and customer data as well as all equipment, systems, networks and software owned or leased by General Audit Tool Ltd..

Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents shall be reported immediately or as soon as possible by dpo@generalauditttool.com.

In your email please describe the incident or observation along with any relevant details.

Whistleblower Anonymous Fraud Reporting

Our Whistleblower Policy is intended to encourage and enable employees and others to raise serious concerns internally so that we can address and correct inappropriate conduct and actions. It is the responsibility of all employees to report concerns about violations of our code of ethics or suspected violations of law or regulations that govern our operations.

It is contrary to our values for anyone to retaliate against any employee or who in good faith reports an ethics violation, or a suspected violation of law, such as a complaint of discrimination, or suspected fraud, or suspected violation of any regulation. An employee who retaliates against someone who has reported a violation in good faith is subject to discipline up to and including termination of employment.

Anonymous reports may be submitted via anonymous Google Form at:
https://forms.gle/MQQW4q2VoELS6XES6

Mobile Device Policy

All end-user devices (e.g., mobile phones, tablets, laptops, desktops) must comply with this policy. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

System level and user level passwords must comply with the Access Control Policy. Providing access to another individual, either deliberately or through failure to secure a device is prohibited.

All end-user, personal (BYOD) or company owned devices used to access General Audit Tool Ltd. information systems (i.e. email) must adhere to the following rules and requirements:

- Devices must be locked with a password (or equivalent control such as biometric)

protected screensaver or screen lock after 10 minutes of non-use
- Devices must be locked whenever left unattended
- Users must report any suspected misuse or theft of a mobile device immediately to the DPO
- Confidential information must not be stored on mobile devices or USB drives (this does not apply to business contact information, e.g., names, phone numbers, and email addresses)
- Any mobile device used to access company resources (such as file shares and email) must not be shared with any other person
- Upon termination users agree to return all company owned devices and delete all company information and accounts from any personal devices

Clear Screen, Clear Desk Policy

Users shall not leave confidential materials unsecured on their desk or workspace, and will ensure that screens are locked when not in use.

Remote Access Policy

Laptops and other computer resources that are used to access the General Audit Tool Ltd. network must conform to the security requirements outlined in General Audit Tool Ltd.'s Information Security Policies and adhere to the following standards:

- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software
- Antivirus software must be configured to detect and prevent or quarantine malicious software, perform periodic system scans, and have automatic updates enabled
- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer
- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access General Audit Tool Ltd. resources
- Use of remote access software is allowable as long as it is provided by the company and configured for multifactor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any General Audit Tool Ltd. system
- Usage of public Wi-Fi is strictly forbidden
- Accessing corporate accounts/system/information from unauthorized devices (e.g. public computer in a business center, hotel, etc.) is strictly forbidden

Employees who do not need to perform engineering tasks(e.g. Sales, Support, Marketing etc.) may be provided with Chromebooks - as the ChromeOS and the device security posture itself is build from the ground up (automatic updates, sandboxing, verified boot, built-in virus protection, data encryption and recovery). Due to security posture of these devices not all of the above rules are required, e.g. additional antivirus software is not mandatory (due to sandboxing and built-in virus protection). Nonetheless employees are still required to stay vigilant, receive and confirm proper cybersecurity training and apply the above rules (where appropriate e.g. do not use public Wi-Fi etc.).

Acceptable Use Policy

General Audit Tool Ltd. proprietary and customer information stored on electronic and computing devices, whether owned or leased by General Audit Tool Ltd., the employee or a third party, remains the sole property of General Audit Tool Ltd. for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of Google Drive for business file storage is required for users of laptops or company issued devices.

Storing important documents on the file share is how you "backup" your laptop.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of General Audit Tool Ltd. proprietary information or equipment. You may access, use or share General Audit Tool Ltd. proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices.

For security and network maintenance purposes, authorized individuals within General Audit Tool Ltd. may monitor equipment, systems and network traffic at any time.

General Audit Tool Ltd. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities with properly documented Management approval. Under no circumstances is an employee of General Audit Tool Ltd. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing General Audit Tool Ltd. owned resources or while representing General Audit Tool Ltd. in any capacity. The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by General Audit Tool Ltd.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which General Audit Tool Ltd. or the end user does not have an active license
3. Accessing data, a server, or an account for any purpose other than conducting General Audit Tool Ltd. business, even if you have authorized access, is prohibited
4. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management shall be consulted prior to export of any material that is in question
5. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, email bombs, etc.)
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home
7. Using a General Audit Tool Ltd. computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws
8. Making fraudulent offers of products, items, or services originating from any General Audit Tool Ltd. account
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes
11. Port scanning or security scanning is expressly prohibited unless prior notification to the General Audit Tool Ltd. engineering team is made
12. Executing any form of network monitoring which will intercept data not intended for the

employee's host, unless this activity is a part of the employee's normal job/duty
13. Circumventing user authentication or security of any host, network, or account
14. Introducing honeypots, honeynets, or similar technology on the General Audit Tool Ltd. network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack)
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means
17. Providing information about, or lists of: General Audit Tool Ltd. employees, contractors, partners, or customers to parties outside General Audit Tool Ltd. without authorization

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company and act accordingly.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of "junk mail", or other advertising material to individuals who did not specifically request such material (email spam)
2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages
3. Unauthorized use, or forging, of email header information
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies
5. Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type
6. Use of unsolicited email originating from within General Audit Tool Ltd. networks or other service providers on behalf of, or to advertise, any service hosted by General Audit Tool Ltd. or connected via General Audit Tool Ltd.'s network

Additional Policies and Procedures Incorporated by Reference

Personnel are responsible for reading and complying with all policies relevant to their roles and responsibilities.

Role	Purpose
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy	To identify organizational assets and define appropriate protection responsibilities.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Data Management Policy	To ensure that information is classified and protected in accordance with its importance to the organization.
Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.
Risk Management Policy	To define the process for assessing and managing General Audit Tool Ltd.'s information security risks in order to achieve the company's business and information security objectives.
Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
Third-Party Management Policy	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

Policy Compliance

General Audit Tool Ltd. will measure and verify compliance to this policy through various methods, including but not limited to ongoing monitoring, and both internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the DPO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the DPO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	2023-03-24	Initial version	Paweł Giętkowski	Robert Baker
1.1	2023-11-21	Annual review	Paweł Giętkowski	Robert Baker

Privacy Policy and Terms of Service

GAT Labs Ltd. is an Irish Limited Company, headquartered at 12 Hume, St. Dublin 2, Ireland. Company No. IE-9693416G.

PLEASE READ THESE TERMS OF SERVICE (THE "TERMS") CAREFULLY. IF YOU ELECTRONICALLY ACCEPT THESE TERMS, EXECUTE AND DELIVER THESE TERMS, OR OTHERWISE USE THE GAT Labs SERVICES OR SOFTWARE (COLLECTIVELY, THE "SERVICE"), YOU AGREE TO BE BOUND BY ALL OF THESE TERMS (THE "AGREEMENT") AS A LEGALLY BINDING AGREEMENT BETWEEN YOU AND GAT Labs, Ltd. ("GAT Labs"). IF YOU DO NOT ACCEPT THE TERMS, YOU ARE NOT PERMITTED TO USE THE SERVICE. If you are entering this Agreement as an employee or representative of your employer, the term "you" includes your employer and any other party on whose behalf you act. If your organization has entered into a separate purchase agreement with GAT Labs, then that agreement supersedes these Terms of Service to the extent that they conflict.

1. Provision of Service.

This Agreement governs your use of the GAT Labs website and GAT Labs provision of its SaaS IT management suite of tools (the "Service") to you. Your use of the website and Service are at all times subject to these Terms of Service and your payment in full of any applicable fees.

2. Software License.

Subject to the terms of this Agreement, GAT Labs grants you a non-exclusive, revocable, non-transferable license to use the Service and any upgrades and updates made available by GAT Labs from time to time, solely during the Term (as defined herein). GAT Labs also grants you a non-exclusive, revocable, non-transferable license to use the accompanying documentation ("Documentation") during the Term in connection with your use of the Service. You acquire no right, title, or interest to the Service, the underlying software, or the Documentation except the limited license described in this paragraph. If you are using the free version of the Service, GAT Labs reserves the right to modify the Service and its availability at any time.

3. Your Systems.

The Service provides information about, and helps you manage, the data in your Google Apps domain (your "Google Domain"). By entering into this Agreement, you agree to provide and allow GAT Labs access to your Google Domain via the Internet for the purposes of providing the Service to you, and you represent and warrant that you have the right to grant this access to GAT Labs. You are solely responsible for the set-up, maintenance, and security of your Google Domain.

4. Software Access.

In order for you to use the Service, you must allow access via APIs (Application Program Interface) to your Google Domain. By subscribing to the Service, you agree that GAT Labs may automatically access your Google Domain via Google APIs. If you disable the API access or otherwise fail to implement any changes required to enable the required API access to GAT Labs, your right to use the Service may be immediately revoked at GAT Labs sole discretion. Should Google in any way change API access or the nature of the API functionality you agree you shall not in any way hold GAT Labs responsible for the failure of all or part of its service.

5. Your Data;

GAT Labs Confidentiality Obligation. In providing the Service to you, GAT Labs will analyze, map and collect meta-data only relating to the data stored on your Google Domain, and the manner in which data is stored and used on your Google Domain ("Customer Meta-Data"). Except as provided in Section 6 of the Terms of Service, GAT Labs does not analyze or collect any information held within the files stored on your Google Domain, and such information does not constitute Customer Meta-Data for the purposes of this Agreement. You agree that GAT Labs may collect, store and modify Customer Meta-Data for the purposes of delivering the Service to you. You represent and warrant that, to the extent required, you have obtained all necessary rights and licenses to the data stored on your Google Domain for use as contemplated by these Terms and that GAT Labs use of such data stored on Customer Systems as set forth herein will not violate any third party rights, including intellectual property and privacy rights You acknowledge that, in relation to the EU Data Protection Directive (also known as SSC 2010), GAT Labs acts as a processor of data ("data subprocessor"). GAT Labs will keep the Customer Meta-Data confidential, will store it exclusively on the Google Cloud Platform, will use it only to deliver the Service to you, will and not disclose it to any third party except GAT Labs employees and contractors who have entered into binding agreements with GAT Labs that

contain non-disclosure obligations equivalent to those set forth in this Agreement. GAT Labs may anonymously aggregate non-identifiable Customer Meta-Data with non-identifiable anonymous meta-data from other GAT Labs customers and third parties to create anonymous aggregated meta-data that does not identify any individual customer or the metrics or information pertaining to any individual customer or its domain ("Aggregated Meta-Data"). GAT Labs will own all rights to Aggregated Meta-Data and has the irrevocable right to maintain, store, use and disclose Aggregated Meta-Data.

6. Full Text Search Scan.

If you use GAT Labs Full Text Search functionality, you acknowledge and agree that: (i) GAT Labs will instruct Google to perform an automated scan of the contents of files stored on your Google Domain (the "Customer Content"); (ii) GAT Labs will not store or retain any Customer Content in its own Google Domain, except to the extent that it constitutes Customer Meta-Data; (iii) you may use the Full-Text Search Services solely for your internal business purposes and in compliance with applicable laws and regulations, including without limitation laws and regulations applying to privacy and personal information; (iv) you are solely responsible for ensuring that only appropriate personnel have access to the Full-Text Search Services and that such personnel have been trained in the proper use of the Full-Text Search Services; and (v) GAT Labs does not guarantee the absolute accuracy of the Full-Text Search Services.

7. Restrictions.

You may NOT: (i) provide access to the Service to third parties, or use the Service for the benefit of third parties; (ii) copy or modify all or any part of the Documentation or distribute it to third parties; (iii) unless otherwise permitted by applicable local law, decompile, decrypt, disassemble, reverse engineer or otherwise discover the source code for the software underlying the Service (the "Software"), or attempt to disable or defeat any locking mechanism within the Software or the Service; (v) modify the Software or Service, incorporate the Software or Service in whole or in part in any other product or create derivative works based on all or any part of the Software or Service; (vi) remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Service; or (vii) export the Software or Service or use the Software or Service in any country other than that in which it was obtained. You acknowledge that the Software and Service are subject to United States export laws and regulations and you shall comply with all such laws and regulations in your use of the Software and Service.

8. Ownership, Non-Disclosure.

GAT Labs owns and will retain all rights, title and interest, including without limitation all copyright, trademark, trade secret, patent and other proprietary rights, in and to the Service, Software, Documentation, Evaluation Data and Aggregated Data (the "Proprietary Materials"). You shall keep confidential and not disclose, sell, lease, transfer, sublicense, dispose of, or otherwise make available the Proprietary Materials or any portion thereof, in source or object code, to any third party other than your employees who need access to the Proprietary Materials in order to use the Service and exercise your license rights granted herein. You agree that dissemination of the Proprietary Materials in breach of this Agreement would cause irreparable harm to GAT Labs for which monetary compensation alone would be inadequate, and GAT Labs is entitled to seek injunctive relief prohibiting any such dissemination, in addition to monetary damages and all other remedies available at law or in equity. This Agreement is NOT a sale of the Proprietary Materials or any copy of them. You obtain only such rights as are expressly provided in this Agreement.

9. User Name and Password.

You will need an individual username and password to use the Service. You must safeguard your username and password and keep them confidential, and you will be responsible for any use of the Service by means of your username and password.

10. Entry by User.

Certain areas of our website and the Service require User entry of certain personal or configuration information. GAT Labs requires that the actual User input such information and that such information be accurate and current.

11. Third-Party Sites.

This Website may from time to time include, for User's convenience, links to third-party sites, which GAT Labs does not own or control. These sites are controlled by third parties and are governed by their own terms of use and privacy policies, not by GAT Labs Terms of Service and Privacy Policy. Such sites may use cookies. However, GAT Labs has no access to or control over these cookies or the information collected by them. If the User has any questions about how such third parties use cookies, the User should contact such third parties directly.

12. Feedback.

Upon request by GAT Labs, you agree to provide GAT Labs with reasonable information about your use and evaluation of the Service, including, without limitation, any errors, logs, usage statistics or problems in the Service and any information reasonably necessary for GAT Labs to evaluate such errors or problems, test results and performance data, information relating to the compliance of the Service with documentation, specifications or functionality and comparison with other software or products (collectively, "Evaluation Data"). Without limiting the foregoing, you irrevocably consent to GAT Labs collection of Evaluation Data and any other information and data relating to your use of the Service, by various means (including without limitation through the Service and through any direct communications between you and GAT Labs), without any further notice to, or consent of, you.

13. Term; Enforcement of Terms; Termination.

This Agreement takes effect when you first subscribe for the Service or otherwise begin using the Service, and continues until terminated as set forth in this Agreement (the "Term"). If you fail to fulfil any of your material obligations under this Agreement, GAT Labs and/or its licensors may pursue all available legal remedies to enforce this Agreement, and GAT Labs may, at any time after your default of this Agreement, terminate this Agreement and all licenses and rights granted to you hereunder. You agree that GAT Labs licensors referenced in the Software are third-party beneficiaries of this Agreement, and may enforce this Agreement as it relates to their intellectual property. This License is effective until terminated. This License will terminate immediately without notice from GAT Labs if you fail to comply with any of its provisions. Upon termination, you must remove all access to the service, and you may terminate this License at any time by doing so.

14. U. S. Government Users.

Pursuant to the policy stated at 48 CFR 227.7202-1, U.S. Government users acknowledge that (i) the Software is commercial computer software, (ii) this Agreement embodies the licenses customarily used by GAT Labs for licenses in Software granted to the public, and (iii) the licenses set forth herein shall apply to all possession, use and duplication of the Software by the Government, except to the extent which such licenses are inconsistent with Federal procurement law. The contractor/manufacturer is GAT Labs Ltd., 12 Hume Street, Dublin 2, D02 XN44, Ireland.

15. Support for Non-Paying Customers.

GAT Labs may, in its discretion, provide you with reasonable assistance with the installation of the Software through its email help address at support@generalaudittool.com. Except for any such assistance, the Service does not include any implementation, helpdesk, support or maintenance services with respect to the Software, nor to any bug fixes, error corrections, updates, upgrades or new versions of the Software (collectively, "Support Services"). The assistance provided by GAT Labs is not bound to any SLAs or SLOs.

16. Limited Warranty and Disclaimer.

GAT Labs warrants that, during the period that you have paid applicable fees and remain in compliance with this Agreement, the Service will operate in substantial conformance with the documentation provided by GAT Labs. GAT Labs are not responsible for the accuracy, security or completeness of the data collected via Google's APIs. GAT Labs accept no responsibility for the accuracy or the validity of the data produced. While every effort is made to ensure the data is timely, accurate and valid, GAT Labs will accept no liability or responsibility for the data or for its accuracy. GAT Labs sole responsibility and your sole remedy for any failure of the Service to conform to this warranty shall be GAT Labs commercially reasonable efforts to remedy any error in the Service so as to conform to the warranty within a reasonable time after you notify GAT Labs of the error, or, in the event that GAT Labs is unable to remedy the error, GAT Labs shall refund to you the fees paid by you, if any, with respect to the period during which the Service failed to operate in accordance with the limited warranty. Neither GAT Labs nor its licensors make any warranties with respect to third-party software included in the Software. EXCEPT FOR THE FOREGOING WARRANTY, GAT Labs PROVIDES THE SERVICE AND SOFTWARE TO YOU "AS IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, STATUTORY, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY ANY GAT Labs EMPLOYEE, REPRESENTATIVE OR DISTRIBUTOR SHALL CREATE A WARRANTY FOR THE SERVICE OR SOFTWARE, AND YOU MAY NOT RELY ON ANY SUCH INFORMATION OR ADVICE. GAT Labs LICENSORS EXPLICITLY DISCLAIM ANY AND ALL WARRANTIES WITH RESPECT TO THE SOFTWARE. IN NO EVENT SHALL GAT Labs BE LIABLE FOR ANY BREACH OF THIS AGREEMENT TO THE EXTENT SUCH BREACH IS OUTSIDE ITS REASONABLE CONTROL

17. Publicity, contact.

Either party may use the other party's name and/or logo (the "Marks") on its website, customer or vendor list (as applicable) or other marketing materials to refer to the relationship between the parties pursuant to this Agreement. All such use shall be in accordance with the usage policies and guidelines of the party owning the Marks and provided in writing to the other party. If the owner of the Marks objects to any such use or wishes to revoke its permission to use its Marks hereunder, the other party shall cease any such use promptly after receiving notification. Neither party's use of the other party's Marks implies or confers any endorsement by either party. From time to time GAT Labs may pass the Administrator's contact details to one or more of its official resale partners with a view to that partner contacting the Administrator directly or may use such contact details themselves, the customer hereby gives consent for the transfer of such contact details for the sole purpose of engaging the customer on the customer's use of the GAT Labs. The customer agrees that the contact details provided to the tool may be used for the purpose of GAT Labs sending reports and or newsletters and or other items of communication.

18. Limitation of Liability.

IN NO EVENT SHALL GAT Labs OR ITS LICENSORS OR ANY OF THEIR RESPECTIVE SHAREHOLDERS, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS OR OTHER AFFILIATES BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES OF ANY KIND (INCLUDING WITHOUT LIMITATION THE COST OF COVER, DAMAGES ARISING FROM LOSS OF DATA, USE, PROFITS OR GOODWILL), WHETHER OR NOT GAT Labs HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS, HOWEVER, CAUSED AND ON ANY THEORY OF LIABILITY ARISING OUT OF THIS AGREEMENT. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. GAT Labs MAXIMUM LIABILITY ARISING OUT OF THIS AGREEMENT AND/OR YOUR USE OR POSSESSION OF THE SOFTWARE, INCLUDING WITHOUT LIMITATION ANY AND ALL CLAIMS COMBINED, WILL NOT EXCEED THE AMOUNT OF THE FEES YOU HAVE PAID FOR THE SERVICE PROVIDED UNDER THIS AGREEMENT.

THE CONSIDERATION TO BE RECEIVED BY GAT Labs HEREUNDER DOES NOT INCLUDE COMPENSATION FOR ASSUMING OR INSURING ANY OF THE RISKS AND LIABILITIES DISCLAIMED BY GAT Labs. THE LIMITATIONS AND DISCLAIMERS PROVIDED IN THIS SECTION ARE INTENDED TO PREVAIL OVER ANY PROVISION HEREIN TO THE CONTRARY.

19. Payment.

Customers will pay GAT Labs according to the fee schedule set in each Schedule of Services. If a Customer's usage significantly exceeds "normal usage," defined as (a) an average of 5000 files per user in the domain and (b) a maximum of 100 audits, policies or notifications per domain and (c) a maximum of 10 scans per day, then GAT Labs reserves the right to reasonably increase fees after a good faith negotiation with Customer.

20. Governing Law.

This Agreement shall be governed by and interpreted in accordance with the laws of Ireland. The United Nations Convention on Contracts for the International Sale of Goods shall not apply. You and GAT Labs agree that the courts of Ireland shall have exclusive jurisdiction over any disputes arising in connection with the Service or this Agreement, and each party hereby submits to the jurisdiction and venue of such courts.

21. Complete Agreement.

Except as expressly provided herein, this Agreement constitutes the entire agreement between you and GAT Labs in relation to the Service, and supersedes all proposals, oral or written, all negotiations, conversations, discussions and all past courses of dealing between you and GAT Labs relating to the Service and Software, and may only be modified in writing signed by you and GAT Labs. You may not assign this Agreement or any right or license hereunder without the prior written consent of GAT Labs. In the event any term of this Agreement is held by a court of competent jurisdiction not to be enforceable, the remaining terms shall survive and be enforced to the maximum extent permissible by law. No waiver of any right or obligation contained herein shall be given except in writing signed by the party against whom the waiver is sought to be enforced.

Data Protection Officer contact details:

dpo@generalaudittool.com