

DATA PRIVACY AGREEMENT for

Lancaster Central School District

This Data Privacy Agreement ("DPA") is by and between the **Lancaster Central School District** ("EA"), an Educational Agency, and **Blooket LLC** ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency (EA):** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means student personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family

Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable student information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law

In order for Contractor to provide certain services ("Services") to the EA pursuant to date services begin 6/8/2022 [date agreement is signed will populate upon signature]; Contractor may receive PII regulated by applicable New York and federal laws and regulations, among them, 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); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part

121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in this DPA. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework.

5. Contractor's Employees and Subcontractors

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to this DPA where the subcontractor will receive or have access to PII are consistent with those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees.
- (e) Contractor must not disclose PII to any unauthorized party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

6. Training

To the extent required by law, the contractor shall ensure that all its employees and subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

7. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its subcontractors retain PII or retain access to PII pursuant to the service agreement. Contractor will automatically delete all PII from its servers after a period of two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks. The EA may use the administrator portal to delete all PII at any time or may request assistance from Contractor to delete PII at any time. The confidentiality and data security

obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon deletion of PII from both active servers and backups. Data Return and Destruction of Data

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period prescribed by this agreement, or as expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. The EA may use the administrator portal to delete PII at any time or may request assistance from Contractor to do so. If not deleted by the EA, Contractor will delete data identified by the EA containing PII from EA accounts from its servers after a period of no more than two (2) years following termination of the subscription, and from all backup servers after two (2) additional weeks.
- (b) With regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Upon request, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data.
- (e) Contractor may retain PII for legal purposes if necessary by statute, court order or subpoena.

8. Commercial or Marketing Use Prohibition

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose, except that teachers may receive email communications regarding product updates or professional development opportunities from which they may opt out at any time.

9. Encryption

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

10. Breach

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if

contact information is provided for the specific mode of delivery), or by registered or certified mail, and must to the extent available, include a description of the Breach which includes theredate of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor’s investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA’s District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Michele Ziegler,
Data Protection Officer/Director of Instructional Technology and Accountability
Lancaster Central School District
177 Central Avenue
Lancaster, NY 14086
mziegler@lancasterschools.org

11. Cooperation with Investigations

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach of data governed by this DPA.

12. Notification to Individuals

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full actual cost of the EA’s notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student’s Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to this DPA, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to this DPA, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for this DPA are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

Contractor Name: Blooket LLC	
Signature:	<u><i>Gregory D. Stewart</i></u> <small>Gregory D. Stewart (Jun 8, 2022 14:30 EDT)</small>
Printed Name:	gregory stewart
Title:	Managing Member
Email:	gstewart@gregstewartlaw.com
Date:	6/8/2022
Lancaster Central School District Data Protection Officer – Michele Ziegler	
Date:	6/9/22
Signature:	<u><i>Michele Ziegler</i></u> <small>Michele Ziegler (Jun 9, 2022 08:40 EDT)</small>

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

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

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Lancaster Central School District is committed to protecting the privacy and security of student protected data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purpose.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices including, but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student protected data elements collected by New York State (<http://www.nysed.gov/data-privacy-security/student-data-inventory>) is available for public review or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student protected data or teacher or principal Annual Professional Performance Review data. Any such complaint must be submitted, in writing, to: Michele Ziegler, Director of Instructional Technology, 177 Central Avenue, Lancaster, New York 14086. Additionally, parents have the right to have complaints about possible breaches of student protected data addressed. Complaints should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234; the email address is "cpo@mail.nysed.gov". The State Education Department's complaint process is under development and will be established through regulations from the department's chief privacy officer, who has yet to be appointed.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Lancaster Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., Family Educational Rights and Privacy Act; Education Law Section 2-d);
3. The duration of the contract, including the contract’s expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to protect the data privacy and mitigate security risks; and
6. Address how the data will be protected using encryption while in motion and at rest.

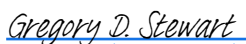
Contractor Name:	Blooket LLC
Signature:	 <small>Gregory D. Stewart (Jun 8, 2022 14:30 EDT)</small>
Printed Name:	gregory stewart
Title:	Managing Member
Email:	gstewart@gregstewartlaw.com
Date:	6/8/2022

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).

<p>Description of the purpose(s) for which Contractor will receive/access PII</p>	<p>The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the district with functionality of the product or services listed above as well as to:</p> <ul style="list-style-type: none"> • To create the necessary accounts to use the Service. • To assess the quality of the Service. • To secure and safeguard personal information. • To access premium features, if applicable. • To comply with all applicable laws on the protection of personal information.
<p>Type of PII that Contractor will receive/access</p>	<p>Check all that apply:</p> <p style="padding-left: 40px;"><input checked="" type="checkbox"/> Student PII</p> <p style="padding-left: 40px;"><input type="checkbox"/> APPR Data</p>
<p>Contract Term</p>	<p>Contract Start Date: 6/8/2022</p> <p>Contract End Date: Agreement remains in effect as long as the account is current and in good standing or upon expiration of the master agreement without renewal, or upon termination of the master agreement prior to its expiration.</p>
<p>Subcontractor Written Agreement Requirement</p>	<p>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)</p> <p style="text-align: center;">Contractor will utilize subcontractors.</p>
<p>Data Transition and Secure Destruction</p>	<p>Upon expiration or termination of the Contract and upon notice from the EA specifying EA accounts and PI, Contractor shall:</p> <ul style="list-style-type: none"> • Securely transfer PII to EA specifically identified by the 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 PII identified by the EA pursuant to an express contract or agreement with the district. Contractor may retain data for legal purposes.
<p>Challenges to Data Accuracy</p>	<p>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 the Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.</p>

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


Contractor Name: Blooket LLC	
Signature:	 <small>Gregory D. Stewart (Jun 8, 2022 14:30 EDT)</small>
Printed Name:	gregory stewart
Title:	Managing Member
Email:	gstewart@gregstewartlaw.com
Date:	6/8/2022

EXHIBIT C - 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 review the following list and 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.**

CONTRACTORS ATTACHED PLAN SHALL INCLUDE THE FOLLOWING:

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.
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.
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.
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.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.
7	Describe your secure destruction practices and how certification will be provided to the EA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 https://www.nist.gov/cyberframework/new-framework



attach company privacy policy here

DATA SECURITY PLAN

10/30/2021

The Blooket LLC Data Security Plan (DSP) describes the survey procedures and data handling protocols that will be implemented to secure study data and protect confidentiality. The plan follows the structure and guidelines established by the National Institute of Standards and Technology (NIST; 800-series).

The DSP considers all known data security and confidentiality protection risks. However, our approaches and specific procedures will evolve as we identify new data security threats and implement improved practices.

1. Purpose

The company restricts access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Rather, its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

2. Scope

2.1 In Scope

This data security policy applies all customer data, personal data, or other company data defined as sensitive by the company. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company is also subject to this policy.

2.2 Out of Scope

Here you define what does not fall under your data security policy. For instance:

Information that is classified as Public is not subject to this policy.

3. Policy

3.1 Principles

The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

3.2 General

- a. Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.
- b. The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.
- c. Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

3.3 Access Control Authorization

Access to company IT resources and services will be given through the provision of a unique user account and complex password.

Role-based access control (RBAC) will be used to secure access to all file-based resources in Active Directory domains.

3.4 Network Access

- a. All employees and contractors shall be given network access in accordance with business access control procedures and the least-privilege principle.
- b. All staff and contractors who have remote access to company networks shall be authenticated using the VPN authentication mechanism only.
- c. Segregation of networks shall be implemented as recommended by the company's network security research. Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation.
- d. Network routing controls shall be implemented to support the access control policy.

3.5 User Responsibilities

- a. All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
- b. All users must keep their workplace clear of any sensitive or confidential information when they leave.
- c. All users must keep their passwords confidential and not share them.

3.6 Application and Information Access

- a. All company staff and contractors shall be granted access to the data and applications required for their job roles.
- b. All company staff and contractors shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.
- c. Sensitive systems shall be physically or logically isolated in order to restrict access to authorized personnel only.

3.7 Access to Confidential, Restricted information

a. Access to data classified as ‘Confidential’ or ‘Restricted’ shall be limited to authorized persons whose job responsibilities require it, as determined by the Data Security Policy or higher management.

4. Technical Guidelines

Access control methods to be used shall include:

- Auditing of attempts to log on to any device on the company network
- Windows NTFS permissions to files and folders
- Role-based access model
- Server access rights
- Firewall permissions
- Network zone and VLAN ACLs
- Web authentication rights
- Database access rights and ACLs
- Encryption at rest and in flight
- Network segregation

Access control applies to all networks, servers, workstations, laptops, mobile devices, web applications and websites, cloud storages, and services.

5. Reporting Requirements

- a. Incident reports shall be produced and handled within the IT Security department or the incident response team where necessary.
- b. Weekly reports detailing all incidents shall be produced by the IT Security department and sent to the CTO when necessary.

6. Ownership and Responsibilities

- **Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.
- **Information Security Administrator** is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.
- **Users** include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees and volunteers.

- **The Incident Response Team** shall be chaired by an executive and include employees from departments such as IT Infrastructure, IT Application Security, Legal, Financial Services and Human Resources.

7. Enforcement

Any user found in violation of this policy is subject to disciplinary action, up to and including termination of employment. Any third-party partner or contractor found in violation may have their network connection terminated.

8. Definitions

This paragraph defines any technical terms used in this policy.

- **Access control list (ACL)** — A list of access control entries (ACEs) or rules. Each ACE in an ACL identifies a trustee and specifies the access rights allowed, denied or audited for that trustee.
- **Database** — An organized collection of data, generally stored and accessed electronically from a computer system.
- **Encryption**—The process of encoding a message or other information so that only authorized parties can access it.
- **Firewall** — A technology used for isolating one network from another. Firewalls can be standalone systems or can be included in other devices, such as routers or servers.
- **Network segregation** — The separation of the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for technical support and another zone for research, each of which has different technical needs.
- **Role-based access control (RBAC)** — A policy-neutral access-control mechanism defined around roles and privileges.
- **Server** — A computer program or a device that provides functionality for other programs or devices, called clients.
- **Virtual private network (VPN)** — A secure private network connection across a public network.
- **VLAN (virtual LAN)** — A logical grouping of devices in the same broadcast domain.