



**Education Law
§2-d Rider**

Board of Cooperative Educational Services
First Supervisory District of Suffolk County
201 Sunrise Highway
Patchogue, New York 11772
(631) 289-2200

New York State Education Law §2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law §2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor signs a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law §2-d, and Trustifi LLC (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law §2-d, and notwithstanding any provision of the attached contract between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time, if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to, student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law §2-d, including, but not limited to:

"Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in §99.3 of FERPA,

-AND-

Personally identifiable information from the records of ESBOCES and/or participating school districts 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record, or display any Protected Data shall comply with New York State Education Law §2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed, or is terminated, Contractor shall return all ESBOCES' and/or participating school districts' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record, or display any ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data, receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency; and
6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of ESBOCES, Education Law §2-d, and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

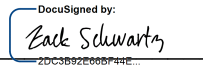
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
 - b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgment, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

NAME OF CONTRACTOR: Trustifi LLC.

BY: Zack Schwartz 

DATED: 07/19/2022

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

See attached Data Privacy Plan and Information Security Policy documents. Eastern Suffolk BOCES Parents Bill of Rights will be added to both documents upon award of RFP.

**EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY**

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians, and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. Eastern Suffolk BOCES wishes to inform the school community of the following rights:

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 maintained by Eastern Suffolk BOCES.
3. State and Federal laws protect the confidentiality of personally identifiable information and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234
CPO@mail.nysed.gov.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into contracts with certain third-party contractors. Pursuant to such contracts, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract

Eastern Suffolk BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

Answer: Student, teacher, and/or principal data will only be used to classify emails for sensitive information or compliance to determine if the emails should be encrypted, blocked, or quarantined.

2. How the third-party contractor will ensure that the subcontractors, persons, or entities with whom the third-party contractor will share the student data or teacher or principal data, if any, will abide by data protection and security requirements;

Answer: There are no third party entities that will have access to student, teacher, and/or principal data within the Trustifi system. All Trustifi systems are proprietary and hosted and managed by Trustifi employees.

3. When the contract expires and what happens to the student data or teacher or principal data upon expiration of the contract;

Answer: Upon contract expiration, student, teacher, and/or principal data will be deleted from the Trustifi system. Upon request from the customer, data can be exported to a third party system.

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 collected; and

Answer: Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway, Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:
Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234
CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security) and the security protections taken to ensure that such data will be protected, including whether such data will be encrypted.

Answer: Student, teacher, and/or principal data is stored within the Trustifi secure private cloud. All data is encrypted at all times.

Third-Party Contractors are required to:

1. Provide training on Federal and State law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to educational records to those individuals who have a legitimate educational interest in such records;
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all State, federal, and local data security and privacy contract requirements will be implemented over the life of the contract; and
9. Provide a signed copy of this Parents' Bill of Rights to Eastern Suffolk BOCES, thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Parents' Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this signed document must be made a part of Contractor's Data Security and Privacy Plan.



DATA PRIVACY PROTECTION PLAN

Version:	0.3
Date of version:	03/14/22
Created by:	Irit Arik
Approved by:	Mark Liapustin
Confidentiality level:	Internal use

Change History

Date	Version	Created by	Description of change
07/30/18	0.1	Irit Arik	Document outline
09/20/18	0.2	Mark Liapustin	Changes, updates
03/14/22	0.3	Mark Liapustin	Audit before ISO27001

Table of contents

1. Summary	3
2. Program plan framework	3
3. GDPR Information Security and Data privacy audit and monitoring plan	5

1. Summary

According to GDPR personal data is critical information that Trustifi needs to protect. Trustifi has adapted and chosen ISO 27001/27002/27018/27017 as data privacy protection program framework to fulfill her obligation to GDPR rule. All these frameworks provide a procedural framework for information security procedures and are customary for these purposes.

Trustifi also covered EU GDPR requirements that are not directly covered by these frameworks such as supporting the rights of personal data subjects: the right to be informed, the right to have their data deleted, and data portability.

Trustifi 's program includes:

- Policies and standards
- Identification and classification
- Data risk and organizational maturity
- Incident response
- Oversight and enforcement
- Privacy and security
- Awareness and education

2. Program plan framework

Policies and standards

- Create update, reconcile data standards, policies, and procedures
- Align and assign data roles and responsibilities
- Determine accountability and decision rights

Identification and classification of data inventory

- Identify structured and unstructured data
- Assess criticality to enterprise and customers
- Understand legal and regulatory obligations
- Maintain inventory and consistent classification

Oversight and enforcement

internal governance of the program, which includes monitoring adherence to policy, remediation, third party vendor management, and when requested, engagement with directors.

- Monitor compliance enforce consistently
- Develop oversight of third-party data protection
- Initiate proactive auditing and reporting
- Enable corporate governance

Data risk, organizational maturity, vulnerability assessments

Trustifi Performs regularly Data Risk Assessments and vulnerability assessments to identify remediate and mitigate new weakness in data security, personal privacy, and Trustifi processes.

Maturity Assessments allow organizations to improve data protection practices by looking at current strengths and weaknesses in relation to a set of data risk principle.

Incident response

- Enterprise-wide data Incident Response Process (IRP) that is the integration with corporate incident response program
- Process for taking corrective action where needed to uphold established data protection standards
- Expanded IRP to cover international requirements
- Enable cooperation with a third party and customer IRPs
- Develop closed-loop corrective action process

Awareness and education

- Effective training, practical documentation and awareness programs
- Development, delivery, and maintenance of collateral needed to educate the workforce, customers, and third-party partners
- Build a network of advocates across the enterprise, partner to implement change

3. GDPR Information Security and Data privacy audit and monitoring plan

	Scope Measurements	Method	Period	Monitoring and review scope	Control
1.	Measure the effectiveness of information security system, and privacy determine and monitor implementation of information security objectives	Meeting with: CEO, Regulation and compliance officer, Information Security officer	Once a year	Information security data privacy	Management review
2.	The effectiveness of the information security system	Reviewing documents and records, interviews and personal observations	Once a year	Implementation processes will be examined	The audit, Monitoring processes
3.	Identifying and measuring gaps from the previous risk assessment management	Interviews with Information owners on core processes	Once a year Ongoing on new /changed processes	Trustifi Performs regularly Data Risk Assessments and vulnerability assessments to identify remediate and mitigate new weakness in data security, data privacy, and Trustifi processes	Risk assessment, DPIA
4.	Helping to discover information security high and medium risk vulnerabilities	BLACK BOX will be performed	Once every 2 years A new service will be checked before being		A penetration test, Code Review

			raised to Production		
5.	Helping to discover information security high and medium risk vulnerabilities		Once a year	The company's processes will be examined in aspects of information flow, access controls, and applicable procedures	Audits to sensitive information, and data privacy
6.	Assistance in measuring the effectiveness of information security training	Phishing e-mails, training	Half a year	Monitoring and checking employee awareness	Checking the effectiveness of information security training
7.	Useful for detecting security events	Access system logs according to the sensitivity of the information	ongoing	Receiving reports from various information security systems Login to systems and check the system: Software updates/system messages	Logging and monitoring of information security systems and sensitive systems, data privacy
8.			Half a year	Password strength, anti-virus updates, patch updates	Checking employees' laptops
9.			Half a year	Antivirus, patches, Hardening	Servers checking
10.			Once a year	Check user Access privileges	User Rights Survey
11.			ongoing		Policies update
12.			ongoing	Check for new sub processors	Subprocessor /Third parties



INFORMATION SECURITY POLICY

Creation date	09/22/2018
Last update date	July 27, 2022
Created by	Irit Arik
Approved by	Mark Liapustin
Confidentiality level	Internal use

TABLE OF CONTENTS

Information Security Policy	1
Introduction.....	4
Information security framework	4
Information security definitions	4
Information security activity in the company is guided by three main principles.....	4
Main purpose and goals of information security activities	4
The overall goals for information security at Trustifi are the following:	4
Security strategy.....	5
The term information security relates to the following basic concepts.....	5
Information security Policy.....	5
Identification of requirements and interested parties	5
Laws Identification and requirements.....	5
Interested parties	6
Statement of Management Intent.....	6
It is the policy of the organization to ensure that information will be protected from a loss of	6
Management goals	7
it will operate in the following ways.....	7
Control and monitoring measures, benchmark achievements	7
Information Security Activities as part of Trustifi commitment to up-to-date information security activities the following is a list of actions to be performed	7
Organizational Structure.....	8
Scope	8
The Information Security Policy applies to all forms of information including	8
Steering committee	8
Appointed Information Security, Compliance and Data Protection Officer	9
Information Security, Compliance and Data Protection Officer.....	9
The responsibilities of the Information Security and Compliance Officer shall include, but not be limited to, the following	9
Employees and Contractors responsibility	10
Data Privacy	10
Data Classification	10
Asset management.....	10
Security Risk Management	11

The following assets should be classified as high-risk systems in any case.....	11
Network scans and penetration tests.....	11
Information Security in HR Management.....	12
Employee Awareness.....	12
Physical and Environmental Security.....	12
Equipment and Media Security.....	12
Audit Trail.....	13
This monitoring activity will focus on two different paths.....	13
Network Management.....	13
Separation of Environments.....	13
Access Control.....	14
Access Permission Management.....	14
REmote Access Control.....	14
Encryption.....	14
Encryption shall be implemented in the following cases.....	15
Systems Maintenance and Development.....	15
Any implementation or upgrade of systems shall include, among others.....	15
Physical security.....	15
Outsourcing.....	15
The contract shall include the following issues.....	15
Anti-Virus.....	16
Secure applications and secure development.....	16
The principle-based approach for application security in Trustifi company includes.....	16
Security Policy Update.....	17
Compliance.....	17
Lawfulness of processing under GDPR.....	17
At least one of these must apply whenever you process personal data.....	17
Validity and document management.....	17

INTRODUCTION

Trustifi holds, processes, and shares personal data, an asset that needs to be suitably protected.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Trustifi information systems and databases are critical resources constituting an asset to the company's activity and management. Therefore, assuring data confidentiality, integrity and availability is the main target for company management and the board of directors.

Trustifi is constantly improving its security governance at all organizational levels. While information security is mainly governed and enforced by Trustifi IT and R&D teams, Trustifi sees the implementation of security measures as a long-term mission for the company, requiring the constant awareness and attention of all employees and the ongoing commitment of management.

INFORMATION SECURITY FRAMEWORK

INFORMATION SECURITY DEFINITIONS

Information security (IS) is a combination of the various actions and measures taken on information systems, to ensure data protection.

INFORMATION SECURITY ACTIVITY IN THE COMPANY IS GUIDED BY THREE MAIN PRINCIPLES

- **Data Confidentiality** – Protection of the data from use by unauthorized personnel.
- **Data Integrity** – Data in databases should always be identical to the source data; however, it may be subject to change according to company needs only by the CTO.
- **Data Availability** – The capability to access data whenever it is needed.

MAIN PURPOSE AND GOALS OF INFORMATION SECURITY ACTIVITIES

Trustifi is committed to safeguarding the confidentiality, integrity, and availability of all physical and electronic information assets to ensure that regulatory, operational and contractual requirements are fulfilled.

THE OVERALL GOALS FOR INFORMATION SECURITY AT TRUSTIFI ARE THE FOLLOWING:

- Ensure compliance with current HIPAA regulations and guidelines.
- Ensure compliance with current GDPR regulations and guidelines.
- Comply with requirements for confidentiality, integrity, and availability for Trustifi employees, customers, and clients.
- Establish controls for protecting Trustifi information and information systems against theft, abuse and other forms of harm and loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, to minimize the risk of security incidents.
- Ensure that Trustifi can continue their services even if major security incidents occur.
- Ensure the protection of personal data (privacy).

SECURITY STRATEGY

Trustifi current business strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the Information Security Policy.

It has been decided that information security is to be ensured by the policy for information security and a set of underlying and supplemental documents. To secure operations at Trustifi even after serious incidents, Trustifi shall ensure the availability of backup procedures, defense against damaging code and malicious activities, system and information access control, incident management and reporting.

THE TERM INFORMATION SECURITY RELATES TO THE FOLLOWING BASIC CONCEPTS

- **Confidentiality:** Information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** Safeguarding the accuracy and completeness of assets.
- **Availability:** Data is accessible and usable upon demand by an authorized entity.

Some of the most critical aspects supporting Trustifi activities are confidentiality and reliability of customer's personal health information (PHI) according to HIPAA law.

Every user of Trustifi information systems shall comply with this information security policy. Violation of this policy and of relevant security requirements will, therefore, constitute a breach of trust between the user and Trustifi, and may have consequences for employment or contractual relationships.

INFORMATION SECURITY POLICY

The IS policy applies to every employee, manager, or service provider of the company, as well as all information systems in use. The company's measures for implementation of this policy include definition of responsibilities and authorities, procedures and regulations, in addition to the use of technological tools.

IDENTIFICATION OF REQUIREMENTS AND INTERESTED PARTIES

LAWS IDENTIFICATION AND REQUIREMENTS

HIPAA is the federal **Health Insurance Portability and Accountability Act** of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

GDPR is the **General Data Protection Regulation** (EU) regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

The primary goal in these laws is to know the interested parties involved in HIPAA and GDPR under Trustifi.

INTERESTED PARTIES

Requirement	Person responsible for compliance	Interested parties
Policy and business environment	CEO	Shareholder/owners of the business
Agreement, NDA, contracts, consents	CEO	Business associate, customers, clients, controllers, individuals
Security clauses in the contracts	CEO	Insurers, referral bodies, customers, clients
HIPAA	Information security, Compliance and Data Protection Officer	Regulators, customer, clients
GDPR	Information security, Compliance and Data Protection Officer	Regulators, customer, clients

A set of policies for information security will be defined, approved by management, published and communicated to Trustifi employees and relevant external parties.

Any changes or updates to Trustifi information security policies will be made only by the VP R&D or the Information Security, Compliance and Data Protection Officer. Any changes to written Trustifi policy documents must also be immediately recorded and denoted by a version update to ensure accuracy and annual review.

STATEMENT OF MANAGEMENT INTENT

IT IS THE POLICY OF THE ORGANIZATION TO ENSURE THAT INFORMATION WILL BE PROTECTED FROM A LOSS OF

- Confidentiality: so that information is accessible only to authorized individuals;
- Integrity: to safeguard the accuracy and completeness of information and processing methods;
- Availability: so that authorized users have access to relevant information when required.

Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, processes and procedures.

The requirements of the Information Security Policy, processes, and procedures will be incorporated into the organization's operational procedures and contractual arrangements.

The organization will work towards implementing the HIPAA and GDPR Law.

Guidance will be provided on what constitutes an Information Security Incident.

All breaches of information security, actual or suspected, must be reported and will be investigated.

Business continuity plans will be produced, maintained and tested.

Information security education and training will be made available to all staff and employees.

Information stored by the organization will be appropriate to the business requirements.

MANAGEMENT GOALS

To meet the goals, set by management on information security

IT WILL OPERATE IN THE FOLLOWING WAYS

- Provide resources for continuous improvement of information security.
- Appoint an Information Security Steering Committee, which will determine the policy of the company and make decisions regarding information security.
- Appoint an Information Security and Compliance Officer who will be responsible for information security methodology in Trustifi and manage all activities related to information security.
- Raise employee awareness to information security issues.
- Integrate information security into the development of new systems.
- Periodic surveys to examine the level of information security.
- Implement advanced information security technologies for monitoring and prevention of information security incidents.

CONTROL AND MONITORING MEASURES, BENCHMARK ACHIEVEMENTS

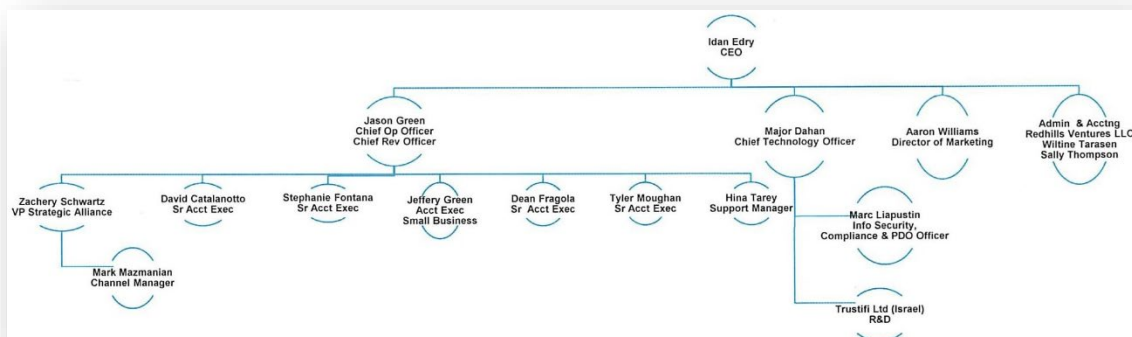
- Management will monitor internal audits.
- Management will monitor the treatment of information security risks.
- Management will monitor risk surveys and penetration tests.
- Management shall ensure periodic compliance audits.
- Executive in charge of information security will require periodic status monitoring and control the various systems.
- Executive Management will survey once a year in accordance with the Management Review Procedure

INFORMATION SECURITY ACTIVITIES AS PART OF TRUSTIFI COMMITMENT TO UP-TO-DATE INFORMATION SECURITY ACTIVITIES THE FOLLOWING IS A LIST OF ACTIONS TO BE PERFORMED

- Penetration testing – annually – outsource
- The penetration tests will be conducted on: the infrastructure and the application
- Vulnerability scan – quarterly – internal
- Employees security awareness – annually – internal
- Application of new security technologies – as applicable
- Security policy reviews – annually

Trustifi is responsible to develop a remediation plan based on the findings of these activities.

ORGANIZATIONAL STRUCTURE



SCOPE

Trustifi is a software-as-a-service (SaaS) company offering a patented postmarked email system that encrypts, tracks, and is the first federally-accepted method of sending legal documents online. The solution provides any company dealing with highly sensitive information with absolute confidentiality, security, and peace of mind. This Information Security Policy outlines the framework for management of Information Security within the organization.

The Information Security Policy, standards, processes and procedures apply to all staff and employees of the company, contractual 3rd parties and agents of the organization who have access to the organization's information systems or information.

THE INFORMATION SECURITY POLICY APPLIES TO ALL FORMS OF INFORMATION INCLUDING

- Hard copy data printed or written on paper;
- Communications sent by chat and electronic mail;
- Stored and processed via servers, PC's, laptops;
- Stored on any type of mobile device;
- Information Security Organizational Structure.

STEERING COMMITTEE

Information security affects all aspects of an organization.

To ensure that all stakeholders affected by security considerations are involved, a steering committee of executives shall be formed. Members of such a committee may include, amongst others, the chief executive officer (CEO) or designee, chief technology officer (CTO), chief information security and regulation officer.

A steering committee serves as an effective communication channel for management's aims and directions and provides an ongoing basis for ensuring alignment of the security program with organizational objectives. It is also instrumental in achieving behavior change toward a culture that promotes good security practices and policy compliance.

APPOINTED INFORMATION SECURITY, COMPLIANCE AND DATA PROTECTION OFFICER

The appointed Information Security and Compliance Officer will be assigned by the company's management and will have the overall responsibility for information security control and regulation.

The Information Security and Compliance Officer holds the responsibility for active implementation of the company's IS policy.

INFORMATION SECURITY, COMPLIANCE AND DATA PROTECTION OFFICER

THE RESPONSIBILITIES OF THE INFORMATION SECURITY AND COMPLIANCE OFFICER SHALL INCLUDE, BUT NOT BE LIMITED TO, THE FOLLOWING

1. Overseeing all ongoing activities related to the development, implementation, maintenance of, and adherence to Trustifi policies and procedures covering the security of, and access to, electronic protected health information in compliance with federal and state laws;
2. Assisting in the identification, implementation and maintenance of regulatory and standard Security Policies and Procedures;
3. Performing and overseeing initial and periodic security risk assessments and conducting related on-going compliance monitoring activities to evaluate advancements in information security technologies and ensure organizational adaptation and compliance;
4. Developing and executing a contingency plan, including applications and data criticality analysis, a data back-up plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures;
5. Overseeing information access controls and maintaining personnel authorization controls and clearance records;
6. Monitoring internal audit controls of system activities and responding to variances;
7. Overseeing security configuration management and security incident procedures, and overseeing device and media controls;
8. Working with legal counsel, consultants and management to ensure that Trustifi has and maintains appropriate security documentation and procedures, reflecting current practices and requirements;
9. Overseeing, directing, delivering or ensuring delivery of timely security training to all members of Trustifi workforce who have access to electronic protected health information and sensitive data;
10. Developing, implementing and monitoring of all vendor and business associate agreements, to ensure that all HIPAA security concerns, requirements and responsibilities are addressed;
11. Reviewing all systems-related information security plans to ensure alignment between these HIPAA Security Policies and Procedures and Trustifi general information security policies and procedures;
12. Maintaining current knowledge of applicable security laws and standards, and monitoring advancements in information security technologies to ensure organizational adaptation and compliance;
13. Evaluating Trustifi security procedures considering any annual guidance published by DHHS pursuant to Section 13401(c) of HITECH, which requires DHHS to annually issue guidance on the most effective and appropriate technical safeguards for use in complying with the security rule;
14. Establishing and administering processes for receiving, documenting, tracking, investigating and taking actions to mitigate or resolve complaints regarding disclosures that are not compliant with these HIPAA Security Policies and Procedures.
15. Cooperating with DHHS in any complaint, review or investigation; and

16. Maintaining records of compliance with these HIPAA Security Policies and Procedures and with all HIPAA requirements.

EMPLOYEES AND CONTRACTORS RESPONSABILITY

All employees are responsible for maintaining the level of IS in the company and behaving in accordance with the company's IS policy. Any employee found to have violated the security policy may be subject to disciplinary action, reporting to the direct manager and further hearing process with HR.

All contractors are responsible for maintaining the IS security level and behaving in accordance with the company's IS policy, and security clauses included in all contracts and SLAs.

All employees and contractors will sign a nondisclosure agreement to ensure information confidentiality.

DATA PRIVACY

The EU's General Data Protection Regulation requires companies to protect the privacy of their EU customers. That means keeping personally identifiable information (PII) safe.

Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can include an IP address, login IDs, social media posts, or digital images. Geolocation, biometric, and behavioral data can also be classified as PII.

A special category of personal data is sensitive data which will now include genetic and biometric data, which if processed will lead to the unique identification of a person. On the other hand, data relating to criminal offenses and convictions are handled separately – criminal law is outside of the EU GDPR's scope. Another type of data that is outside of the GDPR's scope is fully anonymized data, since no individuals can be identified from it.

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

DATA CLASSIFICATION

All data developed, managed, processed, stored or transmitted by the company is classified, excluding public information defined as such by law, or other information defined as non-classified by the Information Security and Compliance Officer

The demands for all data classification, preservation, duplication, extension, or deletion will be defined by the CTO and/or the Information Security, Compliance and Data Protection Officer.

ASSET MANAGEMENT

The organization's assets will be appropriately protected. All assets (data, information, software, computer and communication equipment, service utilities and people) will be accounted for and have an owner.

Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

SECURITY RISK MANAGEMENT

The company will perform a risk assessment for each of its information systems, products, and interfaces, as part of an information security risk assessment survey. The survey should define the sensitivity of each system and address all potential risks.

Risk assessment surveys shall be performed at least once every year and shall be updated according to business and infrastructure changes, or according to the Information security, Compliance and Data Protection Officer.

THE FOLLOWING ASSETS SHOULD BE CLASSIFIED AS HIGH-RISK SYSTEMS IN ANY CASE

- PHI (personal health information)
- PII (personal identifiable information)
- Trustifi algorithm
- Trustifi code
- Credit card Information
- Personal data classification

NETWORK SCANS AND PENETRATION TESTS

The Information Security and Compliance Officer will initiate risk surveys and penetration tests for different systems in the company. High-risk systems will be tested at least once every year or following major system changes. Other systems will be tested at different time periods according to their sensitivity, and at the Information Security and Compliance Officer's discretion.

Surveys will be based upon analysis of business processes and will examine the efficacy of protection measures in place within the company, in addition to the security level of applications and of the infrastructure.

- Once every year, following major system changes or in accordance with risk assessments, the Information Security and Compliance Officer will initiate infrastructure and application penetration tests, to examine the system's resistance to internal and external security risks.
- Once every year, and following major changes, the Information Security and Compliance Officer will initiate internal and external network vulnerability scans of information systems that are open to public communication connections.
- Once every year, the Information Security and Compliance Officer will initiate a network scan to locate wireless unauthorized or unprotected networks enabling access to the company's network.

Annual external vulnerability scans, as mentioned above, shall be carried out by a qualified external third-party, while avoiding conflicts of interests, and taking the obligatory cautionary measures.

The Information Security and Compliance Officer will be responsible for documentation of the network scans and penetration tests findings and will ensure that suitable measures are allocated to address the findings within a reasonable period. After completion, the VP R&D will initiate a quality analysis process to make sure all rectification measures were implemented.

INFORMATION SECURITY IN HR MANAGEMENT

To minimize the risks stemming from the lack of employee awareness, human error, action repudiation, and deliberate malicious acts the company shall implement its information security principles into all HR processes.

To minimize the risk of attacks from internal sources, all candidates for positions that have access to confidential data will undergo a background check, within the constraints of local laws, to validate information provided by candidates. This shall apply to all external party employees, as well.

EMPLOYEE AWARENESS

The Information Security and Compliance Officer shall formulate the information security training for all company employees. The training shall provide and validate that employees have the appropriate knowledge about information security risks and company policies and procedures.

Information security training will take place upon hiring, and at least annually. All employees shall confirm in writing, by signing off, that they read the IS policies.

PHYSICAL AND ENVIRONMENTAL SECURITY

Every work area containing information systems will be classified to a security level, based on the accessible information assets in the area.

To each area, a specified access list of authorized personnel or groups shall be defined. In general, higher classification will demand a smaller number of authorized employees.

The authorization list will be updated with every change of employee function.

Access control measures shall be implemented for all work areas in accordance with the area's classification level, ensuring access is permitted only to authorized personnel.

EQUIPMENT AND MEDIA SECURITY

Handling and management of media containing classified information shall be defined by the Information Security and Compliance Officer. Instructions for handling portable computers and devices shall also be defined by the Information Security and Compliance Officer.

All portable media devices (laptops, mobile devices and external USB storage) must be scanned by Anti-Virus on connection.

The extraction of any equipment or media containing classified information to external parties will follow the Information Security and Compliance Officer's instructions. In addition, a detailed registration of any extracted equipment will be conducted.

The CTO shall insure any equipment intended for maintenance or destruction does not contain any sensitive or classified information.

Physical layouts, including documents and paperwork, will be handled according to the Information Security and Compliance Officer's instructions. The company will erase, shred, or destroy by other means all classified unused information layouts.

AUDIT TRAIL

Audit trails will be used to monitor any successful or failed attempts to perform unauthorized actions in the company's information systems.

THIS MONITORING ACTIVITY WILL FOCUS ON TWO DIFFERENT PATHS

- Retrospective analysis of logs and audit trails in systems and security measures.
- Online tracking of unauthorized activities in the company's network and servers, using various security products.

The types of events monitored, saved, and analyzed, as well as audit trails, will be defined for each system separately. The documentation files will be secured from any unauthorized access or change.

Logs are maintained for at least 90 days in the Event Log.

Ad-hoc monitoring will be done periodically by CTO.

NETWORK MANAGEMENT

The connection of external parties to/from the company network shall be performed through a limited number of secured entrance points. Any other network connection will be prohibited.

Network segregation will be implemented using logical and physical measures of segregation and connection limitations.

Measures for control and screening of incoming and outgoing communication shall be implemented.

Access to the company's servers from outside the company shall be possible only through a secure connection.

Databases containing classified information shall not be accessible to unauthorized users. Access to these DBs will only be possible through secure mediating company computers.

SEPARATION OF ENVIRONMENTS

The production environment will be separated from other environments (QA, development) through physical and logical measures.

Access to the production environment shall be permitted using specific permissions according to the company's authorization policy.

Any data derivation from the production environment to other environments shall be authorized by the Information Security and Compliance Officer, whilst ensuring the environment is properly secured according to the derived information's security classification.

Data and system transfer from the development environment to the production environment shall be performed in a controlled manner, according to procedures, to prevent any harm to data in the production environment.

ACCESS CONTROL

The company shall apply tools for access control management for the information systems and applications. These tools shall contain identification and audit trail measures.

User authentication will be based upon a unique ID related to the user. User authentication shall be based at least on a combination of a username and password. Any remote access to high-risk systems will obligate the use of a strong authentication measure. These measures will apply to company employees as well as other external users.

Access to web-based management interfaces will be encrypted.

ACCESS PERMISSION MANAGEMENT

Access permissions to the company's systems will be applied on a "need to know" basis, for application, DB, operating system, and communication equipment.

Permission segregation shall be applied between regular and administrative users. There will be no administrator permission for a regular user account. Specific administrative user accounts will be used for system management and administration.

Permissions will be allocated based on "permissions profiles" and recorded in the Data Access Record, Company Equipment & Approvals document.

Access permissions shall be examined periodically to ensure appropriate access permissions allocation to functions.

Permission and authorization management will be performed via an automated access control system.

REMOTE ACCESS CONTROL

Any remote connection to the company's information systems shall be performed on a secure end-to-end encrypted connection.

Remote access shall be approved only in accordance with a substantiated need.

ENCRYPTION

All sensitive information shall be encrypted throughout the entire lifecycle including transmission, processing, and storage of the information.

The encryption shall be implemented according to well-known industry standards as well as in accordance with the company's encryption policy.

ENCRYPTION SHALL BE IMPLEMENTED IN THE FOLLOWING CASES

- Any classified information transferred outside the company's network.
- Any classified information saved locally on laptops.
- Encryption of all system access and DB passwords.
- Encryption of all classified data/fields in sensitive applications or databases.

SYSTEMS MAINTANANCE AND DEVELOPMENT

In any process of system development or upgrade, security must be considered. Information security shall be applied by the known standards and regulations.

ANY IMPLEMENTATION OR UPGRADE OF SYSTEMS SHALL INCLUDE, AMONG OTHERS

- System design: Design of security parameters, such as: protocol usage, passwords, permissions, encryption, storage, and other related parameters.
- System construction: Implementation of all security requirements from system design.
- QA: The performing of security QA during development and acceptance tests.
- System implementation: Secure and approved acceptance and installation, while integrating IS personnel in the process.
- System modifications: The company shall take into consideration security issues during any modification or change to the information systems.

PHYSICAL SECURITY

All physical and environmental security must be appropriate to the building or site involved, reviewed and supported by a Risk Assessment.

- Network computer equipment will be housed in a specially controlled and secure environment with restricted access.
- Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
- All visitors to secure Network areas must be authorized.
- Entry controls
- The Information Security and Compliance Officer will maintain a list of the authorized personnel who can access the secured area(s).

OUTSOURCING

Any communication with an external party, which involves external party employee exposure to the company's information, shall be based on a contract and an appropriate due diligence process.

THE CONTRACT SHALL INCLUDE THE FOLLOWING ISSUES

- Definition of the scope of responsibility for each of the parties to the agreement, including sub-contractors' service level agreements (SLAs).
- Duties concerning confidentiality, information security, and emergency situations.
- Arrangements for the termination of the agreement and for resolving disputes.

Exposure of external parties to company data and systems shall be limited and on a “need to know” basis.

Remote access of external employees to the internal network shall be authorized by the Information Security and Compliance Officer.

A preliminary risk assessment shall be conducted to examine all risks stemming from connections to the external party. The relevant security measures will be defined by the Information Security, Compliance and Data Protection Officer according to the risk assessment survey.

ANTI-VIRUS

All workstations, mobile devices must have an anti-virus/phishing/spyware installed.

This shall be updated automatically via the AV server or the Internet.

SECURE APPLICATIONS AND SECURE DEVELOPMENT

THE PRINCIPLE-BASED APPROACH FOR APPLICATION SECURITY IN TRUSTIFI COMPANY INCLUDES

- Knowing the threats.
- Researching new security solutions and implementations.
- Securing the network, host and application.
- Incorporating security into the software development process S-SDLC.
- S-SDLC Process map the security activities above:
- Requirements Gathering
 - Security Requirements
 - Setting up Phase Gates
 - Risk Assessment
- Design
 - Identify Design Requirements from security perspective
 - Architecture & Design Reviews
 - Threat Modeling
- Coding
 - Coding Best Practices
 - Perform Static Analysis
- Testing
 - Vulnerability Assessment
 - Fuzzing
 - Manual and automatic
- Deployment
 - Server Configuration Review
 - Network Configuration Review

SECURITY POLICY UPDATE

The company's IS policy shall be examined and updated once every year or in accordance with major changes in the computerized systems, regulatory instructions, or security risks.

The policy shall be updated by the appointed Information Security and Compliance Officer and approved by management.

After the updating of the IS policy, all relevant functionalities should be notified of the changes made (employees, partners, contractors or any other relevant parties).

COMPLIANCE

Trustifi must comply with current HIPAA and GDPR regulation, as well as other external guidelines and policies.

LAWFULNESS OF PROCESSING UNDER GDPR

The lawful bases for processing are set out in Article 6 of the GDPR.

AT LEAST ONE OF THESE MUST APPLY WHENEVER YOU PROCESS PERSONAL DATA

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Trustifi has reviewed the purposes of her processing activities, and selected consent and contract as the most appropriate lawful basis (or bases) for her activities.

VALIDITY AND DOCUMENT MANAGEMENT

This document is valid as of 09/22/2018.

The owner of this document is the Information Security, Compliance and Data Protection Officer who must check and, if necessary, update the document at least once a year.