Lorem
IPSUM

INFORMATION SECURITY WHITEPAPER

LOREM IPSUM

Version 2021/1.0

SAFECED SAMPLE

SAFECED SAMPLE

SAFECED SAMPLE

Introduction

This paper outlines LOREM IPSUM's approach to security and compliance for products and services. This whitepaper focuses on security including details on organizational and technical controls regarding how LOREM IPSUM protects first, second and third party data.

Information Technology (IT) is an integral and critical component of LOREM IPSUM's (LOREM IPSUM) daily business. LOREM IPSUM has policies in place to ensure that its IT resources efficiently serve the primary business functions, provide security for LOREM IPSUM and partners' electronic data, and comply with federal and other regulations. IT resources include hardware (computers, servers, peripherals), software (licensed applications, operating systems), network equipment (routers, firewalls, wiring), and IT personnel. The integrity of all IT resources is extremely important to the successful operation of LOREM IPSUM's business.

All computer equipment, peripherals, and software are LOREM IPSUM property and are provided for business purposes. Proper use and control of computer resources is the responsibility of all employees. Intentional or reckless violation of established policies or improper use of LOREM IPSUM computers will result in corrective action up to and including termination. Employees should also be aware that any work completed on LOREM IPSUM computers is subject to monitoring and review, and they should not expect their communications to be private.

SAFECED SAMPLE

Definitions

2FA: Two Factor Authentication

AWS: Amazon Web Services

Anti-Spoofing: A technique for identifying and dropping units of data, called packets, that have a false source address.

Antivirus: Software used to prevent, detect, and remove malicious software.

CTO: Chief Technology Officer

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Electronic mail (e-mail): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email spoofing: The forgery of an email header so the message appears to have originated from someone other than the actual source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation to provide sensitive data or perform an action such as processing a wire transfer.

Inbound filters: A type of software based traffic filter allowing only designated traffic to flow towards a network.

Proprietor: owner within the LOREM IPSUM organization

Quarantine: Suspicious email messages may be identified by an antivirus filter and isolated from the normal mail inbox.

SPAM: Unsolicited e-mail, usually from Internet sources. It is often referred to as junk e- mail.

Virtual Private Cloud (VPC): A private cloud computing environment contained within a public cloud.

SAFECED SAMPLE

Security Policies

It is the policy of LOREM IPSUM to use IT resources in a cost-effective manner that safeguards member data and promotes accuracy, safety, Information , and efficiency. The aim is to comply with all federal and other regulations and to protect the integrity of the private and confidential member and business data that resides within LOREM IPSUM's technology infrastructure. To achieve this goal, LOREM IPSUM implements the following security policies and strategies to secure its systems.

1.0 Data Management Policy

LOREM IPSUM collects and stores data of its users and partners and it includes and is not limited to individual information, customers, business contacts, employees data and other organizations data.

The Company Data Protection Policy refers to LOREM IPSUM's commitment to treat information of employees, customers, stakeholders, and other interested parties with the utmost care and confidentiality.

LOREM IPSUM gathers, stores and handles data fairly, transparently and with respect towards individual rights.

SAFECED SAMPLE

1.1 Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to LOREM IPSUM.

Who is covered under the Data Protection Policy?

LOREM IPSUM Employees and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, the policy refers to anyone LOREM IPSUM collaborates with or acts on its behalf.

This data management policy therefore provides guide on how data is governed and ensures LOREM IPSUM:

- Complies with data protection law and follows good practice.
- Protects the rights of customers, staff, and partners.
- Is transparent about how it stores and processes data.
- Protects itself from the risks of a data breach.
- Clearly outlines responsibilities and disciplinary consequences.

1.2 Policy elements

It is LOREM IPSUM's policy not to collect, process or store personal identifiable information in raw form. In cases where personal identifiable information processing or storage is required, data must be one-way digitally hashed such that it is no longer identifiable. This hashing process is done with the full cooperation and knowledgement of all interested parties.

Data shall be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Data shall not be:

- Communicated informally
- Stored for more than the contractually required time period
- Transferred to any other organization, state or entity
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

SAFECED SAMPLE

1.3 Actions

To exercise data protection LOREM IPSUM is committed to:

- Restrict and monitor access to all production data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyber attacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

1.4 Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

1.5 Data Protection Standards

In order to achieve the above objectives, LOREM IPSUM has put the following measures to ensure the data management measures are well met:

1.6 Compliance Requirements

LOREM IPSUM is CCPA (California Consumer Privacy Act) and GDPR (General Data Protection Regulation) compliant. LOREM IPSUM is committed to disclose what personal information it has about persons and what it does with that information, to delete personal information and not to sell personal information. Users also have the right to be notified, before or at the point where personal information is collected, be on the know of the types of personal information that is collected and what may be done with that information.

1.6.1 Storage of Personal Information

All personal information must be stored in encrypted format using one-way SHA256 encryption hashing. LOREM IPSUM's issued equipment that are used to accessing one-way encrypted personal information, must also be well configured and with encrypted disks as per the Access Control Policy in section 4.0.

1.6.2 Data Backup

LOREM IPSUM's Database Administrator (DBA) must ensure that:

- The backup and recovery procedures are documented and meet data proprietor's requirements.
- LOREM IPSUM uses AWS based backup and recovery tools with automated rules expressing the backup schedule, frequency, and backup window. These procedures are well tested and the data is securely stored in the AWS cloud with enterprise level security procedures.

SAFECD
SAMPLE

1.6.3 Logging and Auditing

LOREM IPSUM's ensures that:

- All logins to operating systems and data systems, successful or unsuccessful, are logged. These logs are retained for at least one year. LOREM IPSUM uses AWS services (CloudWatch) to generate log data, such as audit logs for access and configuration changes. In addition to AWS log data; web servers, applications, and operating systems all generate log files in various formats. This enables LOREM IPSUM to properly trace changes and conduct audits needed to protect its data.
- All database objects with protected data have auditing turned on where technically possible.
- All audit logs are regularly reviewed by knowledgeable and independent individuals appointed by the data proprietor to meet the data proprietor's requirements. These requirements and the review process are documented.

1.6.4 Data Encryption

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. To ensure that data is only accessible to the intended users, we ensure that:

- The data is transferred in a secure form and only through a secure network (SSL) and protocol (https). This is exclusive for all platforms.

- Sensitive information such as passwords are stored in encrypted format
- Connection to the data system is encrypted.
- Key management procedures for decrypting backups are documented, available to more than one person and approved by the data proprietor within LOREM IPSUM. The keys are securely managed under AWS Key Management Service (KMS). AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect the keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
- The protected data elements within the database are documented.

SAFECED SAMPLE

1.6.5 Change Management

- Change management procedures are documented and meet the data proprietor's requirements.
- Change management controls are in place to log all changes to the production database.

1.6.6 Database Encryption Key Management

- Key management procedures for decrypting backups are documented, available to more than one person and approved by the data proprietor.
- For data subject to disclosure that is encrypted at storage, the means to decrypt is available to more than one person and approved by the data proprietor.
- Backup stores data in an encrypted format, and the tapes do not store the plain text encryption keys necessary to decrypt the backups.

1.6.7 Data System Security

- LOREM IPSUM's production systems are AWS hosted in a private VPC with a default block all traffic firewall and a NAT gateway to ensure only whitelisted traffic is permitted. This ensures that the data is housed in a secured, locked and monitored environment that prevents unauthorized entry, access or theft.

1.6.8 Application Policy

LOREM IPSUM utilities Serverless Systems and security is handled by AWS serverless security services and this includes deployment access control, API authorization, role based functions and VPS network security procedures.

- Destination systems (application/web servers) receiving protected data are secured in a manner commensurate with the security measures on the originating system. All servers and clients meet minimum security standards.
- All servers, applications and tools that access data systems are documented. Master list of all IT equipment is available.
- Configuration files and source code are locked down and only accessible to required resources on a need-to-know basis. All access is managed in a role based style.

- Application code is reviewed for security vulnerabilities in an automated fashion.
- No "Spyware" is allowed on the application, web or data systems.

1.6.9 Storage of Card Payments Data (PCI-DSS Requirement)

LOREM IPSUM does not collect or store card payments data. Card payments are not processed through any of its systems and PCI-DSS certification is not required.

1.6.12 Responsibilities

LOREM IPSUM maintains well documented procedures on employees responsibilities with respect to access and authorization rights. LOREM IPSUM's employees are well trained and informed about its security standards and measures put in place to secure data.

SAFECD SAMPLE

2.0 Business Continuity

A business continuity plan (BCP) outlines how LOREM IPSUM will continue operating during an unplanned disruption in service.

2.1 Scope

The following measures have been put in place for the Engineering team and other technical individuals to ensure LOREM IPSUM systems recovery is guaranteed during disruption in service.

2.2 Backup Policy

LOREM IPSUM uses Amazon Web Services (AWS) tools such as S3 to manage all the backup and versions. AWS S3 guarantees 99.999999999% (11 9’s) data durability. A data version control system is in place such that at least the latest 2 versions of data are stored at any given time. All data versions can be deleted permanently upon request. Data is replicated in at least 2 AWS availability zones.

2.3 Recovery Policy

Through the AWS systems, LOREM IPSUM is able to seamlessly recover to previous versions incase of catastrophic loss of data. The engineering team members are well trained and conversant with what is required during the recovery process. Because of the multiple availability zones, LOREM IPSUM is able to guarantee recovery in case a problem is only affecting a particular zone.

SAFECED SAMPLE

2.4 Leadership and responsibility

2.4.1 Recovery Team Descriptions

The CTO is the primary responsible party for initiatiing, and ensuring recovery plan is implemented. The Director of Engineering is secondarily responsible in case the CTO is not available.

2.4.2 Communication and Notifications Plans

LOREM IPSUM is committed to maintaining communication through any business continuity events. For external communications, email notifications will be used to keep the stakeholders (users, personel, partners) updated on the progress. The organization will let the stakeholder know of the incident, and progress on the recovery plan.
For internal communication, the team will continue communicating securely through Slack.

2.4.3 Team Contacts

Please refer to section “Contact and responsibility chart” for details on focal personals and teams for each assignment.

2.5 Recovery Plan Phases

2.5.1 Define Disaster Occurrence and declaration of disaster

In case of a disaster, the focal personals will make formal announcements as per the internal and external communication policy (section 7.0).

2.5.2 Define plan activation

LOREM IPSUM has laid down procedures for data recovery, and this includes and not limited to activation of alternate sites operations, activation of data recovery, and restorations from backups. Each team is expected to act as per these procedures for faster turnaround times during a crisis.

2.5.3 On-line Access to systems strategy (Remote plan)

To also ensure team members are able to conduct their activities during critical hours, all team members needed for recovery are able to access internal systems via secured and encrypted using the company provided laptops. Access roles have been configured and well tested through AWS where they can access data. 2FA is enabled for all critical systems.

2.6 Systems Monitoring

LOREM IPSUM systems are under 24/7 monitoring. LOREM IPSUM uses tools such as Uptime Robot to ensure the team gets notified in real time incase of any downtime. This is critical for the team to be able to plan and act fast in case of incidents.

SAFECED SAMPLE

3.0 Human Resource

3.1 Code Of Conduct

Hiring contracts detail code of conduct and clear instructions for safeguarding sensitive information. Every employee is provided with a copy of the HR policy and every new hire signs an agreement to abide by the code of conduct. Both the company and the new employee sign a Mutual Non-Disclosure Agreement (MNDA) which is legally binding. Employees must sign that they understand and will comply with company policies.

3.2 Recruitment

During recruitment, all employees are verified before extending offers. Comprehensive background check is performed. The company maintains detailed identification documents for both on-site and remote team members. The employee files are stored in the cloud securely and a version is kept by HR (CTO)

3.3 Training

The employees are trained during the on-bording phase. The training includes security policies awareness and measures put in place to safeguard company's data. The onboarding officer ensures that employees can securely access work systems from home or from other locations if needed. Proper accounts are set up and adequate training conducted on data, access, and network policies.

3.4 Violations

Violation of any of these policies may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Any employee who violates these policies shall be subject to removal. Additionally, individuals are subject to loss of LOREM IPSUM Information Systems access privileges and may be subject to civil and criminal prosecution.

An orderly exit process exists to equip employees to operate securely and use information appropriately, and ensure that access privileges change is well handled when a user's relationship with the organization changes. This information is provided by the onboarding officer and signed off by the employee. Legal action against violators can be initiated where applicable.

SAFECED SAMPLE

4.0 Access Control

4.1 Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of LOREM IPSUM's entire corporate network. As such, all LOREM IPSUM employees, including contractors and vendors with access to LOREM IPSUM systems, are responsible for taking the appropriate steps, as outlined below, to secure their passwords.

This policy applies to all personnel who have, or are responsible for, an account or any form of access that supports or requires a password on any system that resides at any LOREM IPSUM facility, has access to the LOREM IPSUM network, or stores any non-public LOREM IPSUM information.

4.1.1 Use of a Secure Password Management System

The team uses a secure password management system to ensure good password quality. All personnel must use the approved password management system (LastPass) to ensure the password construction requirements are met.

4.1.2 Construction Requirement

LOREM IPSUM maintains the following password construction requirements. Password must:

- Be a strong password that is auto-generated by the password management
- Be a minimum length of twenty (20) characters on all systems,
- Not be the same as the User ID
- Must have at least 1 special character
- Must have at least 1 numeric character

4.1.3 Password deletion requirement

All passwords that are no longer needed shall be deleted or disabled. This process is handled by application sun-setting and employee off-boarding procedures.

4.1.4 Password Protection Standards

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential LOREM IPSUM information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, "my family name").

SAFECED SAMPLE

- LOREM IPSUM passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with LOREM IPSUM.

4.2 Access Control Policy

4.2.1 Two factor authentication (2FA)

LOREM IPSUM has provided secure log-on access to it's solution. A two factor authentication (2FA) is required, in addition to the basic username and password form. LOREM IPSUM uses a password management system (LastPass), and all entry points to systems have 2FA set up.

4.2.2 Role-based Control System

No single user owns all the rights. The CTO is the only super user in the company. All other employees are given controlled access rights based on roles.

4.2.3 Remote Access Users

Secure VPC where access is controlled via roles with 2FA enabled and configured only to the approved devices.

4.2.4 Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.3 Physical security

Physical security is a form of data protection policy that ensures information devices and facilities where data can be accessed are well protected. LOREM IPSUM ensures security of its facilities and devices by ensuring the following are met.

4.3.1 Access to Facilities

LOREM IPSUM offices are under 24/7 CCTV monitoring. Authorized personnel required to request access through the company's issued key card devices. Entries to the facilities are logged at every entry and exit.

SAFECED SAMPLE

4.3.2 Equipment Inventory

The company maintains a detailed master list of all IT equipment including laptops provided to the employees. For each device, separate super user accounts are set up and hard-drives encrypted. No data is allowed to be stored locally.

4.3.3 Penalties

Personals must use the company's approved devices during work. Use of own devices is prohibited. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

SAFECED SAMPLE

5.0 Change Management

Change Management is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The Change Management Process begins with the creation of a ticket within the LOREM IPSUM work management platform. It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties

Ensuring effective change management within the company's production environments is extremely important in ensuring quality delivery of services.

SAFECED SAMPLE

Key Goals

- The goal is to establish clearly defined best practice processes to ensure compliance with the security policies requirements.
- Improve efficiency through the use of automated tools
- Improve communication through automated escalations and notifications
- Ensure proper level of approvals
- Reduce risk associated with completing changes
- Reduce the impact of changes on the IT and business organizations

Scope

The following solutions are covered in this change management policy

- Software systems developed and deployed by LOREM IPSUM
- Systems infrastructure and configurations
- Workflow base softwares used by LOREM IPSUM for easy operations of its business

5.1 Change management process

All system changes within the company are documented in the company's selected technology platform. Retain AI code base is versioned using a Git based version system and infrastructure configurations changes are governed through an Infrastructure-as-code system. Docker is used primarily during testing, staging, and production deployment. Use of Docker makes systems testing easier and guarantees deployments to work well as they have been tested.

The following are the standard steps we use for most change managements:

- **Formally Request a Change**. All requests for change documented through the company selected change management tool e.g Github issues tracker.
- **Categorize and Prioritize the Change**. The project manager will assess the urgency and the impact of the change on the infrastructure, effort, end user productivity, and budget.

- **Analyze and Justify the Change**. The project manager works with the change requester and the change initiator to develop specific justification for the change and to identify how the change may impact the infrastructure, business operations, and budget. The participants use this information to further research and develop an extensive risk and impact analysis. When completing the analysis of the change, the project manager must ensure they consider the business as well as the technical impacts and risks.
- **Approve and Schedule the Change**. The project manager approves submitted changes requests. Developers will create git pull requests that are well tested and implemented as per the change request assessments.
- **Plan and Complete the Implementation of the Change**. This process includes testing and deployment of the change request, and then completing the change in a manner that will minimize impact on the infrastructure and end users.
- **Post-Implementation Review**. A post-implementation review is conducted to ensure whether the change has achieved the desired goals. Post-implementation actions include deciding to accept, modify or back-out the change; contacting the end user to validate success;

SAFECED SAMPLE

5.2 Assigning the Change Priority

The project manager will have authority to adjust the priority level as required to meet the business needs.
There are four levels of Change priorities which include:

- Emergency – A change that, if not implemented immediately, will leave the organization open to significant risk (for example, applying a security patch).
- High – A change that is important for the organization and must be implemented soon to prevent a significant negative impact to the ability to conduct business.
- Routine – A change that will be implemented to gain benefit from the changed service.
- Low – A change that is not pressing but would be advantageous. Note: Emergency changes must be kept to an absolute minimum due to the increased risk involved in implementing them.

5.3 Approval & Deferral of Change Items

Authorization of a change item occurs after the change is reviewed and depends on the priority of the item as described in the table below.

Change Level	Approval	Notes
Emergency	Approval Required	Emergency

High	Approval Required	Emergency
Routine	These changes bypass the approval process.	This are standard operating procedures
Low	Approval Required	Non-Emergency

5.4 Business Risk and Impact Analysis

The Risk Assessment is used to create a change recommendation to ensure that any risk to the business has been identified and mitigated.
We conduct risk assessment based on the following key criterias:

5.4.1 Risk type assessment by Severity and Impact

Tasks are prioritized based on severity. Using a scale of 1-10, issues are categorized and items with high impact and severity are prioritized.

Risk Type	Severity	Mitigation	Severity after mitigation
Example: Bug fix	5	Task to performed	1

SAFECED SAMPLE

6.0 Incidents management

This policy defines the requirement for reporting and responding to incidents related to LOREM IPSUM information systems and operations. Incident response provides LOREM IPSUM with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

6.1 Policy Details

6.1.1 Monitoring systems

LOREM IPSUM has configured and deployed monitoring systems for all production systems. The engineering team and all focal personnels are notified in realtime on the company's official Slack on the occurrence of an incident.

6.1.2 Incident Response and Recovery

Generally, every incident is critically evaluated and we use change management procedures to fix it.

- A security incident response capability has been developed and implemented for all information systems that house or access LOREM IPSUM controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:
    - Preparation
    - Detection
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
- To facilitate incident response operations, responsibility for incident handling operations will be assigned to the required engineering team. If an incident occurs, the members of this team will be charged with executing the incident response plan and as per the change management policies and procedures. To ensure that the team is fully prepared for its responsibilities, all team members have been trained in incident response operations.
- Incident response plans will always be reviewed and documented based upon the results of previously conducted tests or live executions of the incident response plan.

7.0 Internal and External Communication

LOREM IPSUM uses internal communication tools such as Slack and email for external communication with other stakeholders.

SAFECD SAMPLE

7.1 External Communication Overview

E-mail at LOREM IPSUM must be managed as valuable and mission critical resources. Thus, this policy is established to:

- Create prudent and acceptable practices regarding the use of information resources
- Educate individuals who may use information resources with respect to their responsibilities associated with such use
- Establish a schedule for retaining and archiving email

7.2 Purpose

The purpose of this policy is to establish rules for the use of LOREM IPSUM email for sending, receiving, or storing of electronic mail.

7.3 Audience

This policy applies equally to all individuals granted access privileges to any LOREM IPSUM information resource with the capacity to send, receive, or store electronic mail.

7.4 Legal

Individuals involved may be held liable for:

- Sending or forwarding emails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission
- Knowingly sending or forwarding an attachment that contains a virus

7.5 Policy Detail

Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on LOREM IPSUM's computer systems. LOREM IPSUM can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal emails, files, and documents – are owned by LOREM IPSUM, may be subject to open records requests, and may be accessed in accordance with this policy.

Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of email attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to LOREM IPSUM systems could

SAFECED SAMPLE

wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.

Anti-spoofing practices have been initiated for detecting spoofed emails. Employees should be diligent in identifying a spoofed email. If email spoofing has occurred, IT must be immediately notified.

Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery.

All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm LOREM IPSUM's reputation. The following activities are prohibited by policy:

- Sending email that may be deemed intimidating, harassing, or offensive.
- Using e-mail for conducting personal business.
- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.
- Sending email using another person's email account, except when authorized to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Using unauthorized email software.
- Knowingly disabling the automatic scanning of attachments on any LOREM IPSUM personal computer.
- Knowingly circumventing email security measures.
- Sending or forwarding joke emails, chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct LOREM IPSUM business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.
- Setting up or responding on behalf of LOREM IPSUM without management approval.

E-mail is not secure. Users must not email passwords, social security numbers, account numbers, pin numbers, dates of birth, mother's maiden name, etc. to parties outside the LOREM IPSUM network without encrypting the data.

E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of LOREM IPSUM, unless appropriately authorized (explicitly or implicitly) to do so.

SAFECED SAMPLE

8.0 Network Security

This policy is to protect LOREM IPSUM's electronic information from being inadvertently compromised by authorized personnel connecting to the LOREM IPSUM production environments, and connections between systems.

The CTO is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information systems security policies, standards, guidelines, and procedures.

Scope

The purpose of this policy is to define standards for connecting to LOREM IPSUM's network from any host. These standards are designed to minimize the potential exposure to LOREM IPSUM from damages, which may result from unauthorized use of LOREM IPSUM resources.
Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical LOREM IPSUM internal systems, etc.
Remote access implementations that are covered by this policy include, but are not limited to, responsibilities, access to AWS VPC, and Authentication mechanisms, etc.

SAFECLD SAMPLE

8.1 Network Security

LOREM IPSUM systems are hosted in a VPC in AWS to guarantee data security. Users can only access the company's production systems through the provided company's laptops. All access to the production VPC is role based and requires the user to authenticate with their keys and a 2FA.
It is a requirement that users must not install network hardware or software that provides network services without LOREM IPSUM the CTO approval. Non-LOREM IPSUM computer systems that require network connectivity must be approved by LOREM IPSUM CTO.

8.2 Remote Access

Secure remote access must be strictly controlled. Control will be enforced with 2FA.
LOREM IPSUM employees, engineers, and contractors should never provide their VPC authentication and access keys to anyone, including family members.
LOREM IPSUM employees and contractors with remote access privileges:

- Have a procedure for registration of devices and approval for wireless communication.
    - For remote access to LOREM IPSUM hardware, all hardware configurations must be approved by the company.
    - The approved devices must only be used for LOREM IPSUM assignments and not for personal use

- Have a set of approved technologies that users must use for wireless connections. Only company provided laptops need to be used by employees. Data is never allowed to be replicated or leave the secure VPC environment.
- Employees have signed private access network agreement or any other form of agreement that safeguard against abuse of the network

8.3 Governing Policies

For effective network security strategy, all the employees have been trained on the following key policies:

- Password Policy
- Access Policy
- Data Management Policies
- Physical Security
- Anti-Malicious Software Policy

8.4 Anti-Malicious Software Policy

The purpose of the Anti-Virus and Malware Protection Policy is to establish principles which must be met to prevent malware from entering the organization environment, to identify and report on malware or suspected malware attacks, and to define appropriate actions to eliminate and recover from malware related incidents. To meet this requirement, at LOREM IPSUM:

- Has a clear requirements on anti-malware softwares activation
- Has a clear requirement on malware reporting and troubleshooting where systems are modularied and separated by design. In case system breach, we are able to purge and rollback as per the incident and change management policy.
- Has a support and responsibility desk. In case of any query, all personnels can directly contact their project managers or directly the CTO.
- Violation of this policy can lead to termination of contract.

SAFECED SAMPLE

9.0 Audit Policy

Systems monitoring and auditing, at Retian AI, must be performed to determine when a failure of the information system security, or a breach of the information systems itself, has occurred, and the details of that breach or failure.

Scope

System monitoring and auditing is used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real time while system auditing looks for them after the fact.
This policy applies to all information systems and information system components of LOREM IPSUM. The following components and policies are evaluated:

- Softwares developed and deployed by LOREM IPSUM
- Workflow Softwares used at LOREM IPSUM to enable ease of operations
- Hardwares - Devices assigned to personnels and network devices
- Physical security requirements
- Accounts and password requirements
- Network and configuration security
- Web servers security
- Email requirements
- Disaster Planning and Recovery
- Change management
- Training

9.1 Internal Audit

Internal Audits shall be conducted regularly by qualified internal personnel on all production systems. All internal audits shall be led and signed-off on by LOREM IPSUM's CTO.

9.2 External Audit

LOREM IPSUM is in the process of contracting a third party vendor for SOC 2 - Type II and ISO 9001-20017 auditing and certification. LOREM IPSUM has previously been audited by various Venture Capitalist firms during its fundraising campaigns. Various business processes were evaluated, stability of the system, and composition of the team

SAFECED SAMPLE

Contact and Responsibility Chart

Assignment	Lead Name	Role	Contact
Primary Recovery Plan Lead		Chief Executive Officer	
Secondary Recovery Plan Lead		Director of Engineering	

SAFECED SAMPLE

Document change versions

Version	Changes	Reviewed by	Approved by
2021/1.0	Initial draft	Name: _____________ Sign: ______________ Date: _____________	Name: _____________ Sign: ______________ Date: _____________

SAFECED SAMPLE