**Security Policy Document**

Prepared for Digital Encode Limited

Prepared by: Olaleke Bamidele  
Cybersecurity Analyst

**Identity Management Policy**

**Purpose**

Our Identity Management Policy aims to establish a comprehensive framework for

effectively managing and controlling user identities, access privileges, and

authentication mechanisms within our organization. This policy aims to provide clear guidelines and procedures for creating, maintaining, and terminating user accounts, as well as enforcing access controls and authentication standards. By implementing robust identity management practices, this policy seeks to minimize the risk of unauthorized access, data breaches, and insider threats. Through strong authentication mechanisms, role-based access controls, and regular access reviews, we strive to ensure that only authorized individuals have appropriate access privileges, protect the confidentiality and integrity of our systems and data, and maintain compliance with regulatory requirements. By prioritizing identity management, we strengthen our overall cybersecurity posture, minimize the potential for security incidents, a nd maintain the trust and confidence of our stakeholders.

**Scope**

The Identity Management Policy applies to all our organization's employees,

contractors, and stakeholders. It encompasses managing and controlling user identities,

access privileges, and auth entication mechanisms within our IT infrastructure. This

policy covers all accounts and credentials to access organizational systems,

applications, and data resources. It sets forth guidelines for user provisioning, access

controls, password management, an d account lifecycle management to ensure

information assets' integrity, confidentiality, and availability. The policy defines

procedures for identity verification, role -based access control, single sign -on, and multi -

factor authentication. It also outlines the responsibilities of individuals involved in identity

management processes, including system administrators, IT managers, and identity

administrators. Compliance with this policy is mandatory for all individuals within the

organization, and any deviati ons or exceptions require approval from the designated

authority responsible for identity management and cybersecurity governance.

**Safeguards**

To achieve the organization's overall mission, and the purpose of this cybersecurity

policy, the organization shall:

ID-01 Maintain a Human Resources (HR) program to manage the organization's

workforce members formally.

ID-02 Maintain a Human Resources Information System (HRIS) to track the

status of each organization's workforce member.

ID-03 Ensure that the orga nization's Human Resources (HR) program performs

background screening for each workforce member.

ID-04 Ensure that the organization's Human Resources (HR) program requires

workforce members to agree to the organization's terms and conditions of

employment or similar appropriate contracts.

ID-05 Ensure that the organization's Human Resources (HR) program includes a

process for workforce members to return physical assets after their work

with the organization.

ID-06 Ensure that the organization's Human Res ources (HR) program includes a

process for workforce members to return information assets after their work with the organization.

ID-07 Ensure that the organization's Human Resources (HR) program includes a

process for workforce members to return authenti cation credentials after their work with the organization.

ID-08 Maintain an inventory of each Identity Provider (IDP) the organization

approves.

ID-09 Ensure that the organization minimizes the number of Identity Providers

(IDPs) it uses and utilizes ce ntralized Single Sign On (SSO) solutions whenever possible.

ID-10 Maintain an inventory of each user account authorized by the Identity

Provider (IDP).

ID-11 Maintain a configuration benchmark for each of the organization's

authorized Identity Providers (IDPs).

ID-12 Ensure that the configuration benchmarks for each of the organization's

Identity Providers (IDPs) do not allow workforce members to share accounts.

ID-13 Ensure that the configuration benchmarks for each organization's Identity

Providers (I DPs) do not allow concurrent account logins.

ID-14 Ensure that the configuration benchmarks for each organization's Identity

Providers (IDPs) do not allow account names to be reused within a defined period of time.

ID-15 Define a process the organization shall use to regularly perform identity

reviews of each of the organization's Identity Providers (IDPs) to ensure only authorized accounts exist in the system.

ID-16 Maintain an identity management system to provision accounts for workforce members once automatically added to the organization's Human Resources Information System (HRIS).

ID-17 Maintain an identity management system to automatically de -provision accounts for workforce members once they are tagged as inactive in the organization's Human Res ources Information System (HRIS).

ID-18 Ensure that the configuration benchmarks for each of the organization's

Identity Providers (IDPs) require strong passwords.

ID-19 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require account lockouts if a defined threshold of failed login attempts is exceeded.

ID-20 Ensure that the configuration benchmarks for each organization's Identity Providers (IDPs) require that passwords be stored encrypted and hashed using salts.

ID-21 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require passwords to be transmitted only when encrypted.

ID-22 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require a process for secure password provisioning by the organization's helpdesk.

ID-23 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require using Multi -Factor Authentication (MFA).

ID-24 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require that unused accounts are automatically disabled after a period of not being used and/or require the use of expiration dates on each acco unt.

ID-25 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging logon events for standard accounts (whether successful or failed).

ID-26 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging access to deactivated accounts.

ID-27 Ensure that the configuration benchmarks for each of the organization's Identity Providers (IDPs) require logging User Behavior Analytics (UBA) events.

**Policy Sanctions**

Non-compliance with this policy may result in disciplinary action in line with our

corporation's human resources procedures. Consequences may range from mandatory

refresher training and written warnings to temporary suspension of remote acces s

privileges and, in severe cases, termination of employment or contractual obligations.

Individuals could be subject to legal consequences under applicable laws if violations

involve illegal activities. These sanctions emphasize the critical importance of

cybersecurity, the individual's role in protecting our digital assets, and the potential risks

associated with policy violations. Enforcement will be consistent and impartial, with the

severity of the action corresponding directly to the seriousness of th e breach.

**Access Management Policy**

**Purpose**

Our Access Management Policy aims to establish a comprehensive framework for

controlling and managing user access to our organization's systems, applications, and data resources. This policy aims to provide clear guidelines and procedures for

granting, reviewing, and revoking access privileges, ensuring that users have the

appropriate level of access based on their roles and responsibilities. This policy seeks to minimize the risk of unauthorized access, data breac hes, and insider threats by implementing effective access management practices. By implementing strong authentication mechanisms, role -based access controls, and regular access reviews, we strive to ensure that only authorized individuals can access sensit ive information, protect the confidentiality and integrity of our systems and data, and comply with regulatory requirements. By prioritizing access management, we strengthen our overall cybersecurity posture, safeguard against unauthorized access, and main tain the trust and confidence of our stakeholders.

**Scope**

The Access Management Policy applies to all our organization's employees,

contractors, and stakeholders. It encompasses managing and controlling user access

privileges to systems, applications, and data resources within our IT infrastructure. This policy covers all accounts and credentials to authenticate and authorize individuals' access. It sets forth guidelines for user provisioning, role -based access control, and segregation of duties to ensure a ppropriate access levels are granted based on job responsibilities and the principle of least privilege. The policy defines user account creation, modification, and termination procedures, as well as password management, session management, and access revo cation. It also outlines the responsibilities of individuals involved in access management processes, including system administrators, IT managers, and access administrators. Compliance with this policy is mandatory for all individuals within the organizat ion, and any deviations or exceptions require approval from the designated authority responsible for access management and cybersecurity governance.

**Safeguards**

To achieve the organization's overall mission, and the purpose of this cybersecurity

policy, the organization shall:

AM-01 Define a process for creating and documenting roles and responsibilities

for each of the organization's workforce members.

AM-02 Ensure that the organization's documented roles and responsibilities for

workforce members consi der the principle of separation of duties when defining roles.

AM-03 Maintain documented Access Control Lists (ACLs) for each computing

system and business application system.

AM-04 Ensure that the organization's documented Access Control Lists (ACLs)

for computing systems and business applications are based on the organization's defined roles for workforce members.

AM-05 Maintain Access Control Lists (ACLs) on computing system objects based on approved documentation, roles, and the principle of least pr ivilege.

AM-06 Maintain Access Control Lists (ACLs) on computing system functions

based on approved documentation, roles, and the principle of least privilege.

AM-07 Maintain Access Control Lists (ACLs) on code repositories based on approved documentatio n, roles, and the principle of least privilege.

AM-08 Ensure that the organization's Access Control Lists (ACLs) enforce

encryption of data at rest on each of the organization's computing systems.

AM-09 Ensure that the organization's Access Control Lists (ACLs) enforce data

encryption in transit on each computing system.

AM-10 Define a process for reviewing the organization's documented Access

Control Lists (ACLs) on a regular basis.

AM-11 Define a process for reviewing the organization's Access Control List

(ACL) documentation on a regular basis.

AM-12 Define a process the organization shall use to regularly review the

organization's group or role membership used by the organization's Access Control Lists (ACLs) regularly.

AM-13 Ensure the organizatio n's information systems log and alert changes to

group or role memberships or configured Access Control Lists (ACLs).

AM-14 Ensure the organization's information systems log and alert changes to group or role memberships or configured Access Control Lists (ACLs).

**Policy Sanctions**

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critica l importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the se riousness of the breach.

**Privacy Management Policy**

**Purpose**

Our Data Privacy Policy aims to establish a comprehensive framework for protecting the privacy and confidentiality of personal and sensitive data entrusted to our organization. This policy aims to provide clear guidelines and procedures for data collection, storage, use, disclosure, and disposal in compliance with applicable privacy laws, regulations, and industry best practices. By implementing effective data privacy practices, this policy seeks to ensure the la wful and ethical handling of personal information, safeguard the rights and privacy of individuals, and maintain the trust and confidence of our customers, partners, and stakeholders. Through robust data protection measures, privacy impact assessments, and ongoing monitoring, we strive to mitigate the risks of unauthorized access, data breaches, and misuse of personal information while fostering transparency, accountability, and compliance in our data handling practices.

**Scope**

The Data Privacy Policy appli es to all our organization's employees, contractors,

vendors, and stakeholders. It encompasses the protection and responsible handling of personal and sensitive information collected and processed by the organization. This policy covers collecting, storing , accessing, transferring, and disposing of personal data in compliance with applicable data protection laws and regulations. It outlines procedures for obtaining consent, implementing security measures to safeguard data, ensuring data accuracy, and respon ding to data subject rights requests. The policy sets forth guidelines for data breach notification, data sharing agreements, and vendor management to protect the privacy and confidentiality of individuals' information. Compliance with this policy is manda tory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for data privacy and cybersecurity governance.

**Safeguards**

To achieve the organization's overall mission, and th e purpose of this cybersecurity

policy, the organization shall:

PRV-01 Maintain a transparent, documented privacy program that documents the

organization's safeguards to address data privacy.

PRV-02 Ensure that the organization's documented privacy progr am defines a

process for performing data processing authorizations (authorizing, maintaining, and revoking).

PRV-03 Ensure that the organization's documented privacy program defines a

process for reviewing, transferring, disclosing, modifying, or deleting data from the organization's information systems for privacy purposes.

PRV-04 Ensure that the organization's documented privacy program defines a process for recording and maintaining an individual's privacy preferences.

PRV-05 Ensure that the organizat ion's documented privacy program defines a

process for recording, maintaining, and reviewing stakeholder goals for data privacy.

PRV-06 Ensure that the organization's documented privacy program defines a process for evaluating the organization's use of da ta for bias.

PRV-07 Ensure that the organization's documented privacy program defines a

process for recording and evaluating data provenance and lineage.

PRV-08 Ensure that the organization's documented privacy program defines a

process for limiting the identification or inference of individuals when

processing data.

PRV-09 Ensure that the organization's documented privacy program defines a

process for replacing attribute values with attribute references in the organization's information systems for priv acy purposes.

PRV-10 Ensure that the organization's documented privacy program defines a

process for informing customers and external business partners about how their data is being used and the organization's privacy goals.

PRV-11 Ensure that the organi zation's documented privacy program defines a

process to obtain feedback from individuals regarding the organization's use of data and the associated privacy risks.

PRV-12 Ensure that the organization's documented privacy program defines a

process to allo w individuals to request data corrections to their data.

PRV-13 Ensure that the organization's documented privacy program defines a process to allow individuals to request data deletions of their data (right to be forgotten).

PRV-14 Ensure that the organization's documented privacy program defines a

process for sharing only appropriate data with third parties.

PRV-15 Maintain a technology platform to record the organization's efforts related

to its data privacy program.

PRV-16 Ensure the organizatio n's privacy record system tracks individuals' stated

privacy preferences.

PRV-17 Ensure that the organization's privacy record system tracks data

correction and deletion requests and the organization's response.

PRV-18 Ensure the organization's privacy record system tracks data disclosures or

sharing personal information with third -parties.

**Policy Sanctions**

Non-compliance with this policy may result in disciplinary action in line with our

corporation's human resources procedures. Consequences may rang e from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable law s if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consisten t and impartial, with the severity of the action corresponding directly to the seriousness of the breach.

**Acceptable Use Standard**

**Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment and

other electronic devices at Digital Encode Limited . These rules are in place to protect

the employee and Digital Encode Limited . Inappropriate use exposes Digital Encode

Limited to cyber risks including virus attacks including ransomware, compromise of

network systems and services, data breach, and legal issues.

**Scope**

This policy applies to the use of information, electronic and computing devices, and

network resources to conduct Digital Encode Limited business or interact with internal

networks and business systems, whether owned or leased by Digital Encode Limited ,

the employee, or a third party. All employees, contractors, cons ultants, temporary, and

other workers at Digital Encode Limited and its subsidiaries are responsible for

exercising good judgment regarding appropriate use of information, electronic devices,

and network resources in accordance with Digital Encode Limited policies and

standards, and local laws and regulation. Exceptions to this policy are documented in

section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other

workers at Digital Encode Limited , including all personnel aff iliated with third parties.

This policy applies to all equipment that is owned or leased by Digital Encode Limited .

**Safeguards**

General Use and Ownership

Digital Encode Limited proprietary information stored on electronic and computing

devices whether owned or leased by Digital Encode Limited , the employee or a third

party, remains the sole property of Digital Encode Limited . You must ensure through

legal or technical means tha t proprietary information is protected in accordance with the

Data Protection Standard.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of

Digital Encode Limited proprietary information.

You may access, use or sha re Digital Encode Limited proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual depart ments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within Digital Encode Limited may monitor equipment, systems, and network traffic at any time, per Infosec's Audit Policy . Digital Encode Limited reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

**Security and Proprietary Information**

All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy . System level and user level passwords must comply with the Password Policy . Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. All computing devices must be secured with a pass word -protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended. Postings by employees from a Digital Encode Limited email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Digital Encode Limited , unless posting is during business duties.

Employees must use extreme caution when opening email attachme nts received from unknown senders, which may contain malware.

**Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from

these restrictions during their legitimate job responsibilities (e.g., systems administrat ion

staff may have a need to disable the network access of a host if that host is disrupting

production services). Under no circumstances is an employee of Digital Encode Limited authorized to engage in any activity that is illegal under local, state, fed eral or international law while utilizing Digital Encode Limited -owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for

activities which fall into the category of unacceptable use.

**System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret,

patent or other intellectual property, or similar laws or regulations, including, but not

limited to, the installation or distribution of "pirated" or other software pr oducts that are

not appropriately licensed for use by Digital Encode Limited .

Unauthorized copying of copyrighted material including, but not limited to, digitization

and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Digital

Encode Limited or the end user does not have an active license is strictly prohibited.

Accessing data, a server, or an account for any purpose other than conducting Digital

Encode Limited business, even if you have authorized access, is prohibited. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.). Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Using a Digital Encode Limited computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. Making fraudulent offers of products, items, or services originating from any Digital Encode Limited account. Making statements about warranty, expressly or implied, unless it is a part of normal job

duties. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account tha t the employee is not expressly

authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping

floods, packet spoofing, denial of service, brute -forcing accounts, and forged routing information for malicious purposes. Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.

Executing any form of network monitoring which will intercept data not intended for the

employee's host, unless this activity is a part of the employee's normal job/duty.

Circumventing user authentication or security of any host, network, or account.

Introducing honeypots, honeynets, or similar technology on the Digital Encode Limited

network.

Interfering with or denying service to any user other than the employee's host (for

example, denial of service attack). Using any program/script/command, or sending messages of any kind, with the intent to

interfere with, or disable, a user's terminal session, via any means, locally or via the

Internet/Intranet/Extranet. Providing information about, or lists of, Digital Encode Limited employees to parties outside Digital Encode Limited .

**Email and Communication Activities**

When using company resources to access and use the Internet, users must realize they

represent the company. Whenever employees state an affiliation to the company, they

must also clearly indicate that "the opinions expressed are my own and not necessarily

those of the company". Questions may be addressed to the IT Department Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages. Unauthorized use, or forging, of email header information. Solicitation of email for any other email address, other than that of the p oster's account, with the intent to harass or to collect replies. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type. Use of unsolicited email originating from within Digital Encode Limited 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, anyservice hosted by Digital Encode Limited or connected via Digital Encode Limited 'snetwork. Posting the same or similar non -business -related messages to large numbers of Usenet newsgroups (newsgroup spam).

**Blogging and Social Media**

Blogging or posting to social media platforms by employees, whether using Digital

Encode Limited ’s property and systems or personal computer systems, is also subject

to the terms and restrictions set f orth in this Policy. Limited and occasional use of Digital

Encode Limited ’s systems to engage in blogging or other online posting is acceptable,

provided that it is done in a professional and responsible manner, does not otherwise

violate Digital Encode Li mited ’s policy, is not detrimental to Digital Encode Limited ’s

best interests, and does not interfere with an employee's regular work duties. Blogging

or other online posting from Digital Encode Limited ’s systems is also subject to

monitoring. Digital Encode Limited ’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Digital Encode Limited confidential or proprietary information, trade secrets or any other material covered by Digital Encode Limited ’s Confidential Information policy when engaged in blogging. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Digital Encode Limited and/or any of its employees. Employees are also prohibite d from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Digital Encode Limited ’s Non-Discrimination and Anti -Harassment policy. Employees may also not attribute personal statements, opinions or beliefs to Digital Encode Limited when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Digital Encode Limited . Employees assume any and all risk associated with blogging. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export -controlled materials, Digital Encode Limited ’s trademarks, logos and any other Digital Encode Limited intellectual property may also not be used in connection with any blogging or social media activity

**Policy Sanctions**

Non-compliance with this policy may result in disciplinary ac tion in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.

**Third -Party Management Policy**

**Purpose**

Our Third -Party Risk Management Policy aims to establish a robust and risk -based

approach for evaluating, selecting, contracting, and monitoring third -party vendors and

partners to ensure the security of our organization's information assets. This policy aims

to provide clear guidelines and procedures for assessing the cybersecurity posture of

third parties, managing vendor relationships, and enforcing contractual obligations

related to security controls and d ata protection. By implementing effective third -party

management practices, this policy seeks to mitigate the potential risks posed by third -

party relationships, safeguard our systems, data, and networks from unauthorized

access and breaches, and protect o ur sensitive information's confidentiality, integrity,

and availability. Through a comprehensive due diligence process, regular monitoring,

and ongoing communication, we strive to establish and maintain a trusted ecosystem of

third-party providers that ali gn with our security standards, regulatory requirements, and

overall risk appetite.

**Scope**

The Third -Party Risk Management Policy applies to all employees, contractors, and stakeholders engaging and collaborating with third -party entities with access to the organization's systems, data, or networks. This policy encompasses the assessment, selection, contracting, and ongoing management of third -party vendors, suppliers, partners, and service providers to protect the organization's sensitive information and maintain the integrity of its cybersecurity posture. It sets forth guidelines and procedures for evaluating third parties' cybersecurity capabilities and practices, including due diligence assessments, contractual obligations, and periodic audits. The policy mandates the inclusion of robust cybersecurity controls and requirements within vendor contracts and establishes mechanisms for monitoring, reporting, and remediation of any identified risks or incidents. Compliance with this policy is mandatory for all individuals involved in third -party management, and any deviations or exceptions require approval from the designated authority responsible for cybersecurity governance.

**Safeguards**

To achieve the organization's overall mission, and the purpose of this cyb ersecurity policy, the organization shall:

TPR-01 Maintain a process for approving each of the organization's third parties that store or process any of the organization's technology systems or data.

TPR- 02 Maintain a Governance, Risk, and Compliance (GR C) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data.

TPR-03 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data maintains a complete inventory of all such third parties.

TPR-04 Ensure that the organization's Governanc e, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organization's technology systems or data documents the demographics of all such third parties (such as bu siness owner, criticality, whether data is shared).

TPR-05 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar platform to document and inventory each of the organization's third parties that store or process any of the organi zation's technology systems or data maintains a complete data inventory of all data stored or processed by such third -parties.

TPR-06 Maintain consistent, appropriate, and approved contract language for each

organization's third parties that store or proc ess any of the organization's technology systems or data.

TPR-07 Ensure that the organization's third -party contract language includes provisions requiring any third party that experiences a significant cybersecurity event (such as a data breach) to promp tly report it to the organization.

TPR-08 Ensure that the organization's third -party contract language includes provisions that all third parties must implement cybersecurity safeguards.

TPR-09 Ensure that the organization's third -party contract languag e includes provisions requiring all third parties to implement a defined set of cybersecurity safeguards, also defining which of those safeguards are

**optional versus mandatory.**

TPR-10 Ensure that each of the organization's third parties that store or proc ess

any of the organization's technology systems or data signs the agreed -upon contract terms.

TPR-11 Ensure that each of the organization's third parties that store or process

any of the organization's technology systems or data is regularly assessed for the appropriate cybersecurity safeguards.

TPR-12 Ensure that each of the organization's third parties that store or process

any of the organization's technology systems or data is monitored for significant cybersecurity events.

TPR-13 Ensure that each o f the organization's third parties that store or process any of its technology systems or data are given an aggregate cybersecurity rating based on their criticality, implementation of appropriate cybersecurity safeguards, and occurrence of significant cybersecurity events.

TPR-14 Ensure that each of the organization's third parties that store or process any of the organization's technology systems or data are appropriately decommissioned when there is no longer a need for the third party to perform such s ervices.

**Policy Sanctions**

Non-compliance with this policy may result in disciplinary action in line with our

corporation's human resources procedures. Consequences may range from mandatory

refresher training and written warnings to temporary suspension of remote access

privileges and, in severe cases, termination of employment or contractual obligations.

Individuals could be subject to legal consequences under applicable laws if violations

involve illegal activities. These sanctions emphasize the critic al importance of

cybersecurity, the individual's role in protecting our digital assets, and the potential risks

associated with policy violations. Enforcement will be consistent and impartial, with the

severity of the action corresponding directly to the s eriousness of the breach.