LOGO

Blank Template

Information Security

Prepared by:			
Management Team:			
Classification:			
		Version: 1.1	

Table of Contents

Document Information

1.1. Document Change History

DATE	VERSION NUMBER	AUTHOR(S)	REVISION NOTES	SECTION ID EDITED

1.2. Document Approval Matrix

NAME	ROLE	SIGNATURE	DATE

SECTION 1

(POLICY STRUCTURE)

1.1 PURPOSE

The purpose of this Information Security Policy is to implement security controls that assist [COMPANY] in protecting its information, and to enable the business to deliver on stated objectives and empower the way in which [COMPANY] operates through information security governance, controls, and effective risk management.

1.2 SCOPE

The [COMPANY] Information Security Policy has been established to protect all information assets, including, but not limited to; paper records, computers including all digitalized information, mobile devices, and network infrastructure components that are owned, leased, or otherwise held, controlled and/or used by [COMPANY]' personnel. This includes, but is not limited to, all corporate information systems facilities, telephone network components and supporting systems, communications networks, and the information stored on, transmitted by and/or processed in these facilities. This policy's requirements apply to all information owned or managed by [COMPANY] no matter its form or location. The policy applies to all directors, officers, employees, contractors, and temporary workers ("personnel") of [COMPANY], its wholly owned and partially- owned subsidiaries and affiliates using its technology assets (collectively, "[COMPANY]"), as well as any parties that interact with, access, or store [COMPANY] information assets.

1.3 OVERVIEW

The policy is designed to (1) ensure the security and confidentiality of information assets, (2) protect against any anticipated threats, known cyberattacks, detected malicious activities or hazards to the security or integrity of information assets, (3) protect against unauthorized access to or use of information assets and computer resources that could result in substantial harm of inconvenience to any customer, employee, or non-employee, and (4) the policy is aligned and meeting the data protection regulatory and compliance requirements for all jurisdictions where it operates.

This policy outlines the process for protecting the confidentiality, availability, and integrity of our information. [COMPANY] defines information as "data associated with meaning and purpose" and information protection incorporates the following criteria:

Confidentiality: [COMPANY],

Integrity:

Availability: [COMPANY]' [COMPANY]

1.4 POLICY COMPLIANCE

The Director, CISO of Cyber & Information Security, will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, security assessments and feedback to the policy owner.

1.4.1 Non-Compliance

Violators of this policy will be subject to disciplinary action up to and including termination of employment. All personnel are required to report any known or suspected policy violation(s) to their manager and/or the Cyber & Information Security Team immediately.

1.4.2 Policy Exceptions

Due to special circumstances, there may be cases where compliance cannot be achieved for reasons beyond [COMPANY]' control. In such cases, an exception to [COMPANY] Information Security Policy, must be requested and submitted by following the organization's Policy Exception Standard. *For specific details, please refer to the Policy Exception Standard located on page 27.*

1.5. APPLICABILITY

This policy is applicable to all [COMPANY]' sectors.

SECTION 2

(END-USER INFORMATION SECURITY POLICY)

ALL EMPLOYEES/NON-EMPLOYEES

Scope:
The following policies and standards outlined below apply to all of [COMPANY]' employees, IT contractors, third-party vendors and business partners that have system access to the organization's network and information assets

END-USER INFORMATION SECURITY POLICY

2.1 USER ACCEPTABLE USE POLICY

Users shall not use, or assist anyone else to use, [COMPANY]' computer resources to perform actions that are reasonably determined by [COMPANY] to be a violation of generally accepted standards of corporate usage.

2.1.1 User Acceptable Use Standard:

Objective:

The purpose of this standard is to outline the acceptable use of computer equipment at [COMPANY]. These standards are in place to protect the employee and [COMPANY]. Inappropriate use exposes [COMPANY] to risks including malware attacks, legal liability, data loss, and compromise of the organization's network systems, business processes and/or services.

[redacted]

[redacted]

2.2 USER SECURITY AWARENESS POLICY

All [COMPANY]' employees, and where relevant [COMPANY]' non- employees, must be provided and complete information security training on a regular basis, no less than annually.

2.2.1 User Security Awareness Standard:

Objective:

The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring all personnel that have access to [COMPANY]' information assets understand their roles and responsibilities as it relates to protecting [COMPANY]' critical data and information.

[redacted]

2.3 USER ACCESS POLICY

[COMPANY] must restrict logical access to only authorized users that require system access to the organization's information assets including, but not limited to computer systems, applications, network devices, end-user devices and third-party cloud solutions. [COMPANY] must have an access control process established, documented and reviewed based on business and information security requirements.

2.3.1 User Access Standard:

Objective:

The purpose of this standard is to provide the security requirements and measurements designed to restrict system access to authorized parties (all personnel), in order to protect customer and business data, the organization's information assets, ensure compliance with relevant statutory, security practices and data privacy regulations.

[COMPANY]'

[COMPANY]'

[COMPANY]'

[COMPANY]'

[COMPANY]

[COMPANY]'

2.4 USER SEPARATION OF DUTIES POLICY

Business functions within [COMPANY] must be appropriately segregated under separate roles, and these roles must be allocated to personnel based on their job responsibilities. Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized, unintentional modification or misuse of the organization's assets.

2.4.1 User Separation of Duties Standard:

Objective:

The purpose of this standard is to provide appropriate security and business measurements that will prevent and mitigate the risk as it relates conflict of interest, wrongful acts (e.g., fraud), abuse/errors, and ensure compliance with relevant statutory, security practices and data privacy regulations.

[COMPANY]'

2.5 USER MALWARE MANAGEMENT POLICY

The need for malware management is to reduce the potential risks to [COMPANY]' information assets, by protecting the software, hardware and data that could be vulnerable to the introduction of malicious code. Therefore, all [COMPANY] personnel must complete their security/awareness training as it relates to understanding their roles and responsibilities, and the various steps required to help mitigate the risks and threats surrounding malware attacks (e.g., phishing emails, ransomware, etc.) against [COMPANY]' network and computer systems.

2.5.1 User Malware Management Standard:

Objective:
Reduce the potential risks to [COMPANY]' information assets, by protecting the software, hardware and data that could be vulnerable to the introduction of malicious code.

[COMPANY];
[COMPANY]'

2.6 PERSONNEL SECURITY POLICY

Policy:
In order to effectively manage [COMPANY]' personnel risks, all personnel management policies must adhere to the personnel security standards, all personnel security standards and procedures will be reviewed and approved with respect to risk assessments and events that may precipitate an update to personnel security policy and procedures. Such events include, without limitation, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, and the standards.

2.6.1 Personnel Security Standard:

Objective:

The objective of this standard is to reduce the business risks associated with effective personnel security measures, by setting forth the standards and procedures to identify, properly screen personnel, assign and review the appropriate personnel to designated business functions given the reviews and risk assessments related to those functions as identified by the organization.

SECTION 3

(INFORMATION TECHNOLOGY SECURITY POLICY)

IT EMPLOYEES/NON-EMPLOYEES ONLY

Scope:
The following policies and standards outlined below apply to all of [COMPANY]' information technology employees, IT contractors, third-party IT vendors that have system access to the organization's network and information assets.

3.1 IT RESILIENCY MANAGEMENT POLICY

Policy:
[COMPANY] must include information security requirements for roles and responsibilities, technical requirements, and impact analyses as part of the business resiliency program for maintaining business functions when systems or processes are compromised.

3.1.1 IT Resiliency Standard:

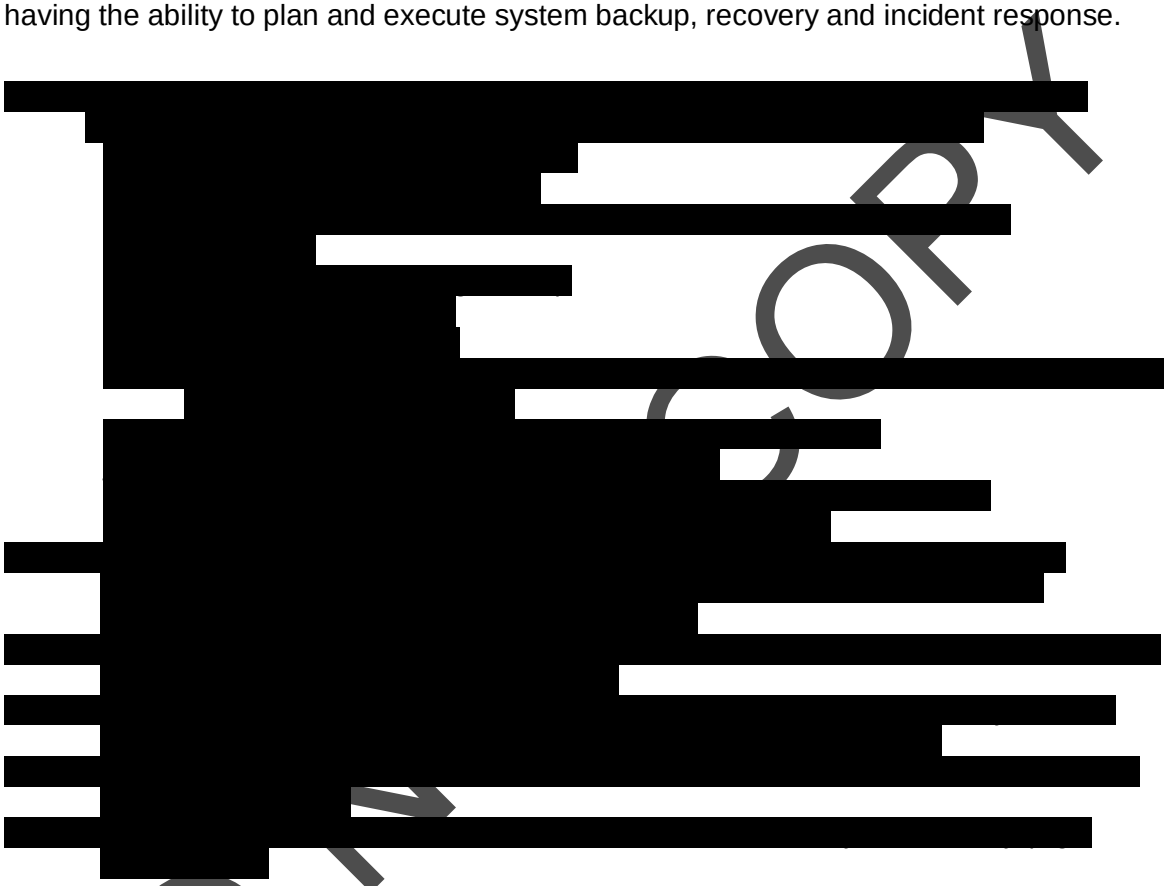
Objective:
The objective of this standard is to ensure the resiliency program has the ability to minimize negative impacts to [COMPANY]' information assets and maintain the organization's critical business processes until regular operating conditions are restored.

3.2 IT ASSET MANAGEMENT POLICY

Policy:
Where appropriate, an inventory of all [COMPANY]' IT assets (e.g., hardware and software) both internal and external must be identified, maintained and updated periodically on an annual basis. Information asset classification must be established based on the potential risk and harm to our customers, business partners and the organization.

3.2.1 IT Asset Management Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by maintaining the appropriate inventory of [COMPANY]' business application's, servers, network hardware and devices, end-user devices (e.g., laptops and smart phones), and SaaS solutions, to ensure the information assets are protected, while having the ability to plan and execute system backup, recovery and incident response.



3.3 IT APPLICATION SECURITY POLICY

Policy:
Access to High and Moderate Disclosure Risk information and data (e.g., PII) must be controlled in all production, test and cloud/SaaS environments by the established application security standards. Information security requirements must be included for system acquisition, development and maintenance.

3.3.1 IT Application Security Standard:

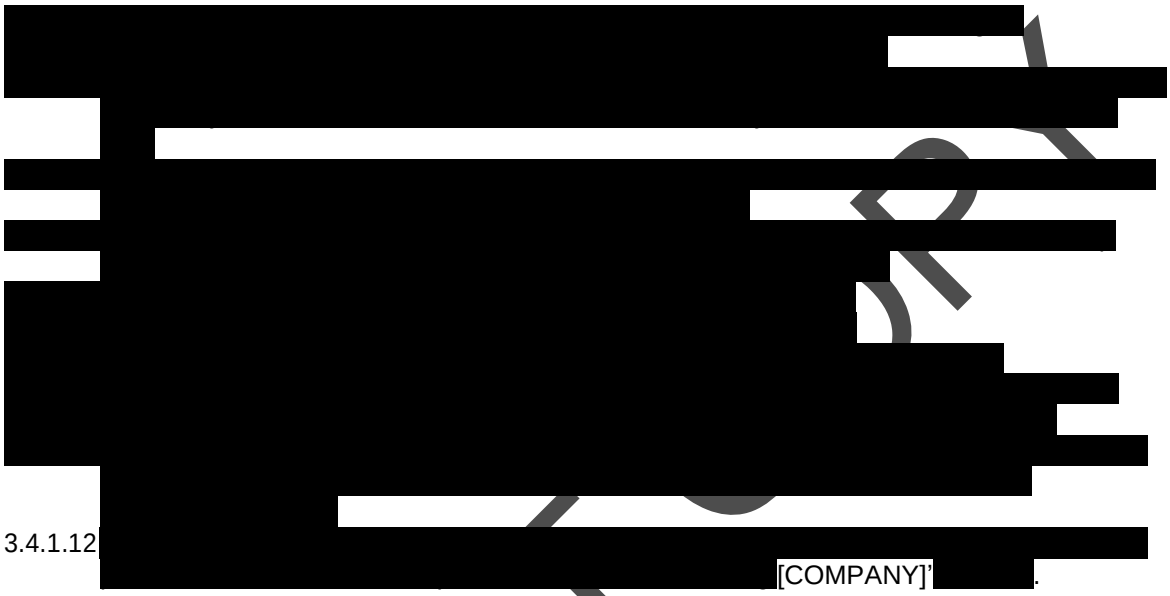
Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring the data confidentiality, integrity and availability to all internal and external hosted [COMPANY] applications.

3.4 IT NETWORK SECURITY POLICY

Policy:
All network and infrastructure devices that store, process and communicate [COMPANY]' data and information must have security controls in place, with the ability to detect and prevent security incidents, as well as having the ability to respond and recover from a security incident.

3.4.1 IT Network Security Standard:

Objective:
The objective of this standard is to ensure the protection of [COMPANY]' information and data that is created, processed, accessed and stored within [COMPANY]' network infrastructure.



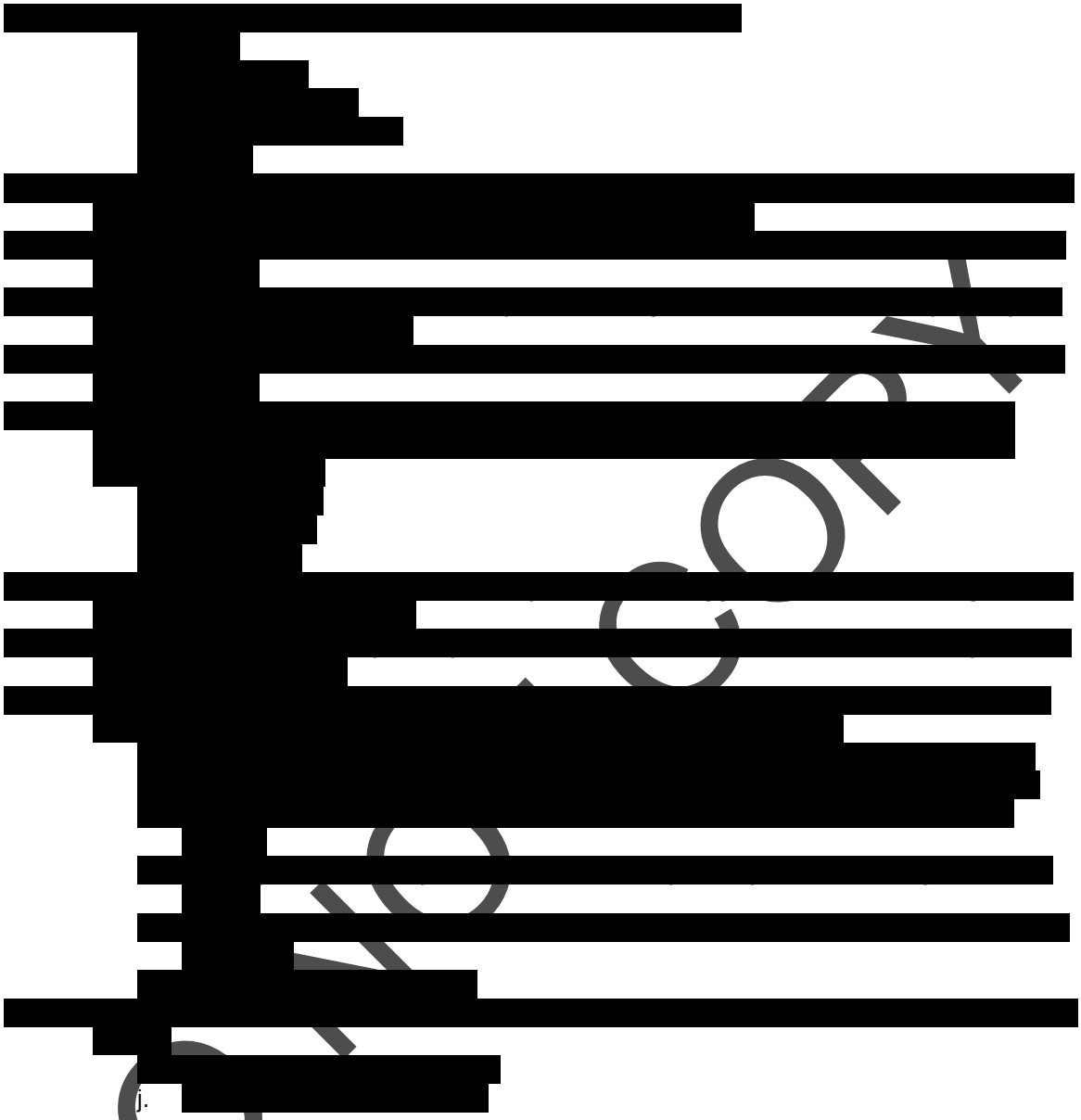
3.4.1.12 [redacted] [COMPANY]' [redacted].

3.5 IT LOGGING AND SYSTEM MONITORING POLICY

Policy:
Where appropriate, business critical IT systems must have ongoing system monitoring in place to collect system and security logs with the ability to produce audit logs of system and user activities, events and potential security incidents.

3.5.1 IT Logging and System Monitoring Standard:

Objective:
The objective of this standard is to detect any malicious system activities or events that could potentially impact the protection of [COMPANY]' data and information.



j.

3.6 IT SECURITY INCIDENT MANAGEMENT POLICY

Policy:
An Information Security Incident Plan must be in place, to detect, prevent, and respond to system related security events that could be potentially malicious, in order to reduce the negative impact and damages to [COMPANY].

3.6.1 IT Incident Management Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring IT security events are captured and remediated in a timely manner.

[redacted]

3.7 IT VULNERABILITY MANAGEMENT POLICY

Policy:
An ongoing technical vulnerability assessment and remediation process must be defined, documented and implemented for all information assets that are considered business critical to the organization or which contain, access and/or transport sensitive information.

3.7.1 IT Vulnerability Management Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by conducting ongoing technical vulnerability assessments and exposing the various system vulnerabilities that could impact the confidentiality, integrity and availability of [COMPANY]' information assets.

[redacted]

.

3.8 IT CHANGE MANAGEMENT POLICY

Policy:
All IT system changes must be controlled and follow the required standards as they relate to the business need, appropriate testing and approvals.

3.8.1 IT Change Management Standard:

Objective:
The objective of this standard is to reduce the risks in terms of unauthorized and unplanned changes made within the IT environment, which could impact the system's availability and interrupt services to the business.

3.9 IT RISK MANAGEMENT POLICY

Policy:
[COMPANY] must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of information assets and computer resources. [COMPANY] must assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of information assets, and assess the effectiveness of the organization's policies, procedures, controls and other arrangements in place to control risks.

3.9.1 IT Risk Management Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring a process is in place to continuously monitor, identify and mitigate cyber security risks to an acceptable level.

3.10 IT VENDOR RISK MANAGEMENT POLICY

Policy:
To ensure the appropriate security of information assets or computer systems accessed by third-party business partners (including external suppliers and service providers), the organization requires that personnel who engage with such third parties must ensure that such third parties adhere to the Information Security Third Party Standard.

3.10.1 IT Vendor Risk Management Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring the proper process is in place to maintain and implement the appropriate level of information security and service delivery.

[redacted]

3.11 IT MEDIA SANITIZATION POLICY

Policy:
[COMPANY] must sanitize all media, paper media, removable media, business mobile computing devices, and information assets prior to disposal, release outside of organizational control, or release for reuse in order to render confidential data permanently non-retrievable by any means:

3.11.1 IT Media Sanitation Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring all obsolete media containing [COMPANY] sensitive data and information is properly disposed of and/or destroyed.

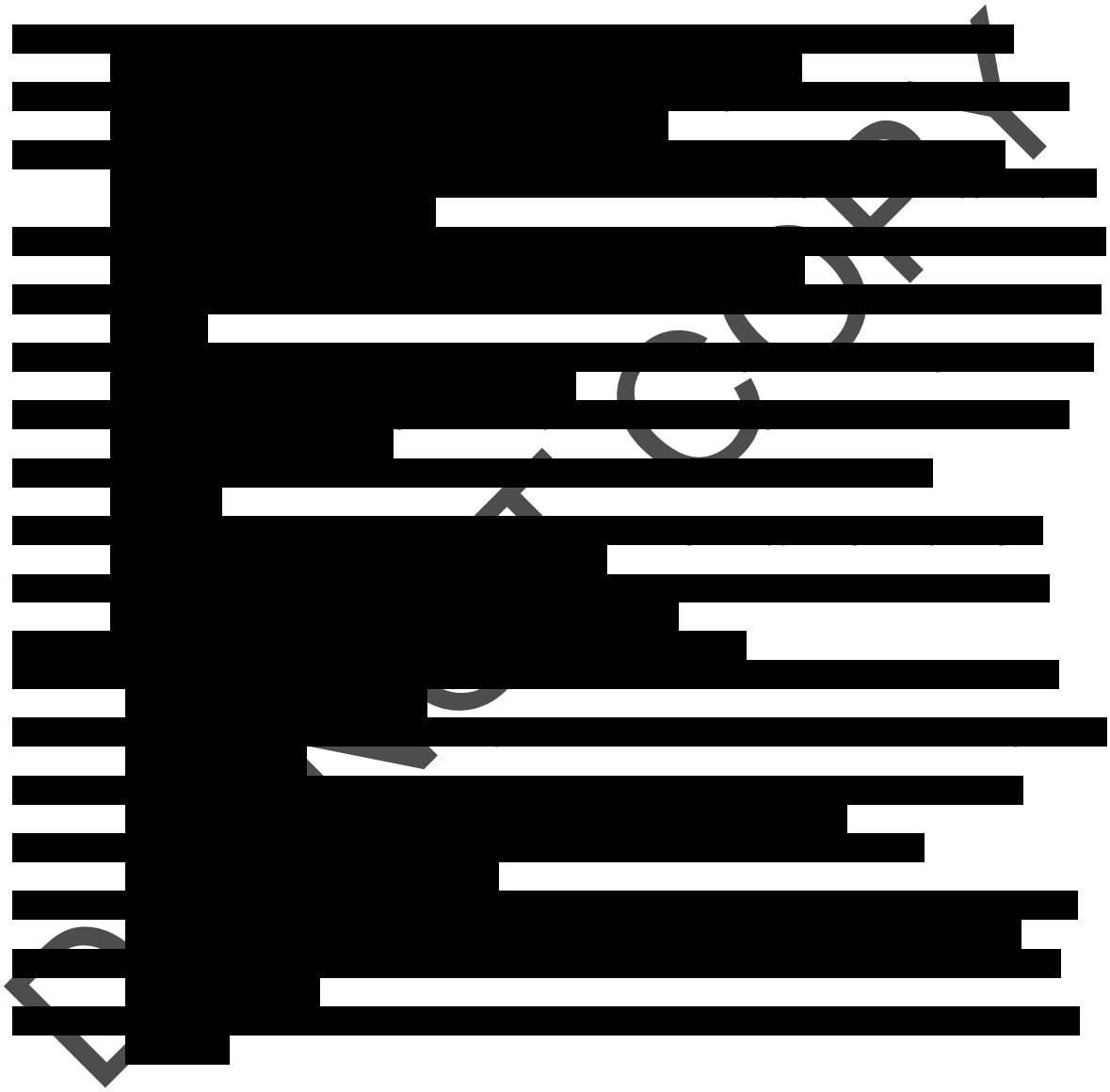
[redacted]

3.12 IT LOGICAL ACCESS POLICY

Policy:
Access control process must be established, documented and reviewed based on business and security requirements to ensure the proper authorization, modification, revocation of access rights, removal of user accounts, access reviews and user activity monitoring to all [COMPANY] critical business systems are in place.

3.12.1 IT Logical Access Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring the assets are secured and protected in terms of managing and executing all system access control tasks consistently and effectively by each information asset custodian.



3.13 IT PASSWORD POLICY

Policy:
All user and system accounts that have access to [COMPANY]' information systems must be adherent to the following password standards.

3.13.1 IT Password Policy Standard:

Objective:
The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by ensuring the assets are secured and protected in terms of managing and executing all system access control tasks consistently and effectively by each information asset custodian.

[redacted]

3.14 IT EQUIPMENT SECURITY POLICY

Policy:
Security perimeters must be in place to protect areas (e.g., server room, data center) that contain information and [COMPANY]' information systems.

3.14.1 IT Equipment Standard:

Objective:
The objective of this standard is to prevent unauthorized physical access, damage and interference to [COMPANY]' information systems and assets.

[redacted]

3.15 IT ENCRYPTION POLICY

Policy:

Where appropriate, all databases, laptops, desktops, servers and mobile devices that store or transfer confidential data and information (i.e., data classified as High or Medium Disclosure Risk) must have the following encryption standards in place.

3.15.1 IT Encryption Standard:

Objective:

The objective of this standard is to reduce the potential risks to [COMPANY]' information assets, by protecting [COMPANY]' critical data and information via cryptographic means

[redacted]

3.16 IT EXCEPTION POLICY

Policy:
All IT policy exception requests must be captured, reviewed and documented via the organization's Policy Exception Standard, with specific details regarding the mitigating factors and compensating controls that will be used to offset the security risk.

3.16.1 IT Policy Exception Standard

Objective:
Due to special circumstances that require deviations from this policy, an exception standard was developed for users to submit, justify and manage their policy exception request.

[redacted]

[redacted]

3.17 IT DATA CLASSIFICATION POLICY

Policy:

In order to effectively secure [COMPANY]' digital data, a classification of each information asset or group of assets must be classified in accordance with the classifications as defined by the organization's classification categories. For addition information, please refer to the Data Classification Grid located on page 31.

3.17.1 IT Data Classification Standards

Objective:

The objective of this standard is to ensure that all of [COMPANY]'s valuable information assets that process, store and transmit digital data both internally and externally are accurately identified, and have the required safeguards in place to mitigate the risks as it relates to regulatory compliance and/or data that could potentially be compromised or leaked.

[redacted]

3.18 IT SYSTEM AND SERVICES ACQUISITION POLICY

Policy:
In order to effectively manage [COMPANY]' systems and technology acquisition risks, all systems and services must adhere to the acquisition standards set forth in Appendix B. Further, all systems acquisitions will be reviewed and approved with respect to consistency with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and standards.

3.18.1 IT System and Services Acquisition Standard

Objective:
The objective of this standard is to ensure that the acquisition of systems and services or the components of systems and services do not create unnecessary or exposure to internal and external threat vulnerabilities.

[redacted]

3.19 IT MALWARE MANAGEMENT POLICY

The need for malware management is to reduce the potential risks to [COMPANY]' information assets, by protecting the software, hardware and data that could be vulnerable to the introduction of malicious code. Therefore, where applicable all IT systems, network devices, etc. within [COMPANY] must have malware protection enabled, updated, and monitored at all times.

3.19.1 IT Malware Management Standard:

Objective:

The objective of this standard is to reduce the potential risks to [COMPANY] information assets, by protecting the software, hardware and data that could be vulnerable to the introduction of malicious code.

[redacted]

APPENDIX A CLASSIFICATION AND TYPE OF DATA GRID

Classification & Type of Data	Type of Security Controls Required
High Disclosure Risk: Information that is considered ***significant business critical*** to the organization's on-going operations and could seriously damage the organization if lost or made public. Such information includes the following but not limited to… [redacted] Information classified as High Disclosure Risk has very restricted distribution and must always be protected. ***Security at this level is the highest possible***	[redacted] ➢
Moderate Disclosure Risk: Information that is considered ***business sensitive*** to the organization's on- going operations and could seriously impede them if made public or shared internally. Such information includes the following but not limited to… [redacted] Such information should not be copied or removed from the organization's operational control without specific authority. ***Security at this level should be very high***	[redacted] ➢
Low Disclosure Risk: Information not approved for general circulation outside the organization where its disclosure would inconvenience the organization or management but is unlikely to result in financial loss or serious damage to credibility. Examples include the following but not limited to … [redacted] Such information should be used with caution if shared outside the organization. **Security at this level is controlled but normal.**	[redacted] ➢

APPENDIX B
SECURITY POLICIES AND NIST STANDARD MAPPING

NIST CSF FUNCTION	NIST CSF Category	NIST CSF Sub Category	Policy #	Page #
IDENTIFY (ID)	**Asset Management (ID.AM)**	ID.AM-1: Physical devices and systems within the organization are inventoried	3.2	14
		ID.AM-2: Software platforms and applications within the organization are inventoried	3.2	14
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	3.2	14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	3.10	22
		ID.BE-1: The organization's role in the supply chain is identified and communicated	3.10	22
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack,	3.1	12
	Governance (ID.GV)	ID.GV-1: Organizational cybersecurity policy is established and communicated	1.2	5
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	1.3	5
		ID.GV-4: Governance and risk management processes address cybersecurity risks	3.9	21
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	3.9	21
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	3.9	21

		ID.RA-3: Threats, both internal and external, are identified and documented	3.9	21
		ID.RA-4: Potential business impacts and likelihoods are identified	3.9	21
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	3.9	21
		ID.RA-6: Risk responses are identified and prioritized	3.9	21
	Risk Management Strategy (ID.RM)	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	3.9	21
	Supply Chain Risk Management (ID.SC)	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	3.10	20
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	3.10	22
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	3.10	22
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	3.10	22
PROTECT (PR)	**Identity Management (PR.AC)**	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	3.12	23
		PR.AC-2: Physical access to assets is managed and protected	3.14	25

		PR.AC-3: Remote access is managed	3.12	23
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	3.12	23
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	3.13	23
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	3.13	25
	Awareness and Training (PR.AT)	PR.AT-1: All users are informed and trained	2.2	9
		PR.AT-2: Privileged users understand their roles and responsibilities	2.2	9
		PR.AT-4: Senior executives understand their roles and responsibilities	2.2	9
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	2.2	9
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	3.12 3.15 3.19	23 26 30
		PR.DS-2: Data-in-transit is protected	3.12 3.15 3.19	23 26 30

		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	3.2	23
		PR.DS-5: Protections against data leaks are implemented	3.5	26
	Information Protection Policies, Processes and Procedures (PR.IP)	PR.IP-2: A System Development Life Cycle to manage systems is implemented	3.18	29
		PR.IP-4: Backups of information are conducted, maintained, and tested	3.1	14
		PR.IP-6: Data is destroyed according to policy	Refer to the Corporate Data Retention Policy	n/a
		PR.IP-7: Protection processes are improved	3.8	20
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	3.6	18
		PR.IP-10: Response and recovery plans are tested	3.6	18
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	3.12	23
	Maintenance/Change Management (PR.MA)	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	3.8	20
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	3.8	20

	Protective Technology (PR.PT):	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	3.5	15
		PR.PT-2: Removable media is protected, and its use restricted according to policy	3.11	21
		PR.PT-4: Communications and control networks are protected	3.4	14
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	3.4	14
DETECT (DE)	**Anomalies and Events (DE.AE): Anomalous activity is detected, and the potential impact of events is understood.**	DE.AE-2: Detected events are analyzed to understand attack targets and methods	3.5	17
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	3.5	17
		DE.AE-4: Impact of events is determined	3.5	17
		DE.AE-5: Incident alert thresholds are established	3.5	17
	Security Continuous Monitoring (DE.CM): **The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.**	DE.CM-1: The network is monitored to detect potential cybersecurity events	3.5	17

		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	3.5	17
		DE.CM-4: Malicious code is detected	3.19	30
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	3.5	17
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	3.5	17
		DE.CM-8: Vulnerability scans are performed	3.7	19
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	3.6	18
		DE.DP-2: Detection activities comply with all applicable requirements	3.5	17
		DE.DP-3: Detection processes are tested	3.7	19
		DE.DP-4: Event detection information is communicated	3.5 3.6	17 18
		DE.DP-5: Detection processes are continuously improved	3.7	19
RESPONSD (RE)	**Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to**	RS.RP-1: Response plan is executed during or after an incident	3.6	18

	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external	RS.CO-1: Personnel know their roles and order of operations when a response is needed	3.6	18
		RS.CO-2: Incidents are reported consistent with established criteria	3.6	18
		RS.CO-3: Information is shared consistent with response plans	3.6	18
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	3.6	18
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated	3.5 3.6	17 18
		RS.AN-2: The impact of the incident is understood	3.6	18
		RS.AN-3: Forensics are performed	3.6	18
		RS.AN-4: Incidents are categorized consistent with response plans	3.6	18
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	3.7 3.5 3.6	19 17 18
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained	3.6	18

		RS.MI-2: Incidents are mitigated	3.6	18
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	3.7	19
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and	RS.IM-1: Response plans incorporate lessons learned	3.6	18
		RS.IM-2: Response strategies are updated	3.6	18
RECOVERY (RC)	**Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.**	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident	3.1 3.6	14 18
		RC.IM-1: Recovery plans incorporate lessons learned	3.1	14
		RC.IM-2: Recovery strategies are updated	3.1	14
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	3.1 3.6	14 18