

Information Security Policy

Topc B.V.

(A company registered in Curaçao with registration number
163568)

Registered Office: Korporaalweg 10, Curaçao

Effective Date: 20.07.2025

1. Introduction

1.1 Purpose:

This Information Security Policy has been formally established by Topc B.V., a company incorporated in Curaçao under registration number 163568, with its registered office located at Korporaalweg 10, Curaçao. In this Policy, the company may be referred to as “the Company,” “we,” “us,” or “our.”

The primary objective of this Policy is to define and uphold a structured and coherent framework designed to ensure the confidentiality, integrity, and availability of all information assets under the Company’s control. It articulates the guiding principles, roles, and procedures that are essential for protecting corporate data and technology resources from unauthorized access, misuse, disclosure, disruption, alteration, or destruction.

Through the implementation of this Policy, the Company seeks to reduce both operational and reputational risks, promote continuity of business operations, and reinforce the confidence of clients, partners, and other key stakeholders by maintaining high standards of information security.

Statement of Alignment

This Information Security Policy has been developed in accordance with the principles and requirements of ISO/IEC 27001. It reflects the Company’s commitment to establishing, implementing, maintaining, and continually improving an effective Information Security Management System (ISMS) to protect the confidentiality, integrity, and availability of information assets.

1.2. Scope:

This Policy is applicable to all individuals and entities who interact with the Company’s information systems and assets. This includes, but is not limited to, employees, contractors, consultants, temporary personnel, and third-party service providers. It encompasses all forms of information and related infrastructure that are owned, processed, or managed by the Company.

The scope of the Policy extends to physical and digital storage systems, internal and external communication networks, and all hardware and software used for operational or administrative purposes. It also includes cloud-based platforms and services, as well as any information that is transmitted, stored, or processed in electronic, physical, or verbal formats.

Furthermore, the Policy applies uniformly across all business units and operational locations of the Company. This includes remote and mobile work settings, thereby ensuring a consistent, organization-wide approach to safeguarding information security.

1.3. Definitions and Terminology

This Policy uses specific information security terms to ensure consistent understanding across the organization. These terms are aligned with internationally recognized standards, including ISO/IEC 27001. Definitions are provided in **Appendix A (Glossary)** for reference. Key terms include, but are not limited to, the following:

- **Information Asset** – Any data, device, or component that supports information-related activities and is valuable to the organization.
- **Confidentiality** – The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity** – The property of safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – The property of being accessible and usable upon demand by an authorized entity.
- **Threat** – A potential cause of an unwanted incident that may result in harm to a system or organization.
- **Vulnerability** – A weakness of an asset or control that can be exploited by one or more threats.
- **Risk** – The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.
- **Control (or Safeguard)** – A measure that is implemented to manage risk, including policies, procedures, practices, or organizational structures.

- **Security Incident** – A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations or information security.
- **User** – Any person who has been authorized to access information or an information system.
- **Access Control** – The process of granting or denying specific requests to obtain and use information and related resources.
- **Asset Owner** – An individual or entity with approved responsibility for maintaining the proper protection and use of an information asset.

Employees and stakeholders are expected to familiarize themselves with these terms to properly understand and adhere to the requirements outlined in this Policy.

1.4. Roles and Responsibilities

All individuals subject to this Policy share a collective responsibility for preserving the confidentiality, integrity, and availability of the Company's information assets. Specific roles are assigned defined responsibilities to ensure the effective implementation, monitoring, and continuous improvement of information security controls across the organization.

Senior Management

Senior management is accountable for supporting and endorsing the Information Security Policy. Their responsibilities include:

Approving the policy and ensuring it aligns with business objectives and regulatory requirements.

Allocating sufficient resources for the implementation and maintenance of information security measures.

Promoting a culture of security awareness throughout the organization.

Information Security Officer (or CISO, if appointed)

The Information Security Officer is responsible for overseeing the information security program, including:

Developing, updating, and enforcing information security policies and standards.

Conducting risk assessments and recommending mitigation strategies.

Monitoring compliance with security policies and reporting on security performance and incidents.

Coordinating responses to security incidents and breaches.

IT Department / Technical Teams

IT personnel are responsible for implementing technical and procedural safeguards, including:

Managing and securing IT infrastructure, systems, networks, and applications.

Ensuring secure configuration, access control, backup, and patch management.

Performing system monitoring, vulnerability scanning, and log analysis.

Responding to technical security incidents and coordinating recovery processes.

Department Heads / Line Managers

Managers must ensure that all personnel within their teams:

- Are aware of and comply with this Policy.

- Complete mandatory security awareness training.
- Report security concerns or incidents in a timely manner.
- Apply appropriate data classification and access control rules within their departments.

Employees and Contractors

All employees, contractors, interns, and temporary staff are expected to:

Comply with all security policies, procedures, and acceptable use guidelines.

Handle Company data responsibly and only access information required for their role.

Immediately report any suspected data breaches, phishing attempts, or policy violations.

Third-Party Service Providers

Third parties who access or process Company data must:

Adhere to contractual and legal information security obligations.

Implement controls that are at least equivalent to the Company's internal standards.

Cooperate in audits or reviews related to their handling of the Company's information assets.

1.5. Risk Management

The Company maintains a formal and structured Information Security Risk Management process to identify, assess, treat, and monitor risks that could affect the confidentiality, integrity, and availability of its information assets, systems, and services.

This process is an integral part of the Company's overall governance and supports informed decision-making, compliance with applicable regulations, and the prioritization of security investments.

Risk Identification

Risks are identified by evaluating internal and external threats, system vulnerabilities, and the potential impacts of security incidents. Sources of risk include, but are not limited to:

Cyberattacks (e.g., phishing, ransomware, DDoS)

Insider threats (intentional or accidental)

Technology failures or misconfigurations

Third-party service disruptions

Regulatory or legal non-compliance

Risk Assessment

Each identified risk is analyzed in terms of likelihood and impact using a qualitative or quantitative methodology. The outcome determines the risk level (e.g., low, medium, high, critical) and helps prioritize mitigation actions.

Risk Treatment

Appropriate risk treatment options are selected based on cost-benefit analysis and business objectives. These may include:

Mitigation – implementing security controls to reduce risk to an acceptable level

Avoidance – modifying or discontinuing risky activities

Transfer – shifting risk to a third party (e.g., via insurance or outsourcing)

Acceptance – consciously retaining residual risk when justified

Risk treatment plans are documented and assigned to responsible individuals for implementation and follow-up.

Risk Monitoring and Review

All risks and controls are reviewed on a regular basis or when significant changes occur in the Company's operations, technology, or threat landscape. Monitoring activities include:

Regular security assessments and audits

Review of incident trends and near misses

Evaluation of control effectiveness

Updates to the risk register

Integration with Business Processes

Risk management is embedded into business planning, procurement, project development, and change management to ensure proactive security considerations throughout the organization.

1.6. Incident Response

All suspected or confirmed information security incidents must be reported immediately to ensure a timely and effective response. Prompt reporting allows the Company to quickly contain any potential threats, minimize damage, and safeguard sensitive information.

The Company follows a structured incident response process consisting of the following key phases:

1. **Identification:**
Employees and systems must promptly identify and report any unusual or suspicious activities that may indicate a security incident. Early detection is critical to preventing further harm.
2. **Reporting:**
Once an incident is suspected or confirmed, it must be reported immediately to the designated Incident Response Team (IRT) or Information Security department using established communication channels such as a dedicated hotline, email, or incident management system.
3. **Containment:**
The Incident Response Team will take immediate steps to isolate and contain the incident to prevent it from spreading or escalating. This may include disconnecting affected systems from the network or applying temporary controls.
4. **Investigation:**
A thorough investigation will be conducted to determine the nature, cause, scope, and impact of the incident. This includes collecting and analyzing logs, system data, and other evidence to understand how the breach occurred.
5. **Eradication:**
After identifying the root cause, the team will remove any malicious code, unauthorized access points, or vulnerabilities exploited during the incident to ensure the threat is completely eliminated.

6. **Recovery:**

Systems and services will be restored to normal operation carefully and securely. Continuous monitoring will be implemented during recovery to detect any signs of recurrence.

7. **Lessons**

Learned:

A post-incident review will be conducted to analyze what happened, evaluate the effectiveness of the response, and identify improvements to prevent similar incidents in the future. Findings and recommendations will be documented and communicated to relevant stakeholders.

The Company emphasizes that every employee plays a vital role in the incident response process by remaining vigilant, reporting incidents promptly, and cooperating fully during investigations.

1.7. Monitoring and Audit

The Company implements continuous and proactive monitoring of its systems, networks, and information assets to detect unauthorized activities, potential security breaches, and anomalies that may indicate threats or policy violations. This monitoring involves:

- **Real-time analysis** of network traffic, system logs, and user activities using automated tools and security information and event management (SIEM) systems to identify suspicious behaviors or incidents promptly.
- **Alerting and escalation protocols** to ensure that detected anomalies are investigated immediately by the appropriate security personnel.
- **Access control reviews** to verify that permissions and user rights align with the Company's security policies and least-privilege principles.

In addition to continuous monitoring, the Company conducts **periodic security audits** to assess the effectiveness and adequacy of its security controls. These audits may be internal or external and include:

- **Vulnerability assessments and penetration testing** to identify weaknesses before they can be exploited.
- **Review of compliance** with applicable laws, regulations, and internal policies.
- **Evaluation of technical controls** such as firewalls, antivirus solutions, encryption, and patch management.
- **Assessment of operational practices** including incident response readiness, user awareness, and physical security measures.

Audit results are analyzed to identify areas for improvement. Findings are reported to management, who are responsible for implementing corrective actions and strengthening the Company's overall security posture.

This systematic approach to monitoring and auditing ensures that the Company maintains a high level of security, promptly addresses risks, and continuously improves its defenses against evolving threats.

1.8. Policy Review and Updates

This Policy shall be reviewed at a minimum on an annual basis to ensure its continued relevance and effectiveness. Additionally, the Policy shall be reviewed and updated as necessary in response to significant changes in business operations, technology infrastructure, regulatory requirements, or in the event of security incidents or audit findings.

The review process shall involve relevant stakeholders, including representatives from Information Security, Legal, IT, and other affected business units. Proposed amendments shall be subject to a thorough evaluation to maintain alignment with the Company's strategic objectives and compliance obligations.

All revisions must receive formal approval from senior management prior to implementation. Upon approval, the updated Policy shall be communicated to all employees, contractors, and relevant third parties to ensure awareness and compliance.

Documentation of the review process, including changes made and management approvals, shall be retained in accordance with the Company's record-keeping policies.

This structured approach to Policy management supports continuous improvement and effective governance of the Company's information security framework.

2. Acceptable Use Standard

2.1 General Use and Ownership

The Company's proprietary information stored on electronic and computing devices, whether owned or leased by the Company, the employee, or a third party, remains the sole property of the Company. The Company must ensure, through legal or technical means, that proprietary information is protected in accordance with the Data Protection Standard.

Employees/contractors have a responsibility to promptly report the theft, loss, or unauthorized disclosure of our proprietary information.

Employees/contractors may access, use, or share our proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.

Employees/contractors are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments 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 the Company may monitor equipment, systems, and network traffic at any time, per Infosec's Audit Policy.

The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The Company classifies all information assets based on their sensitivity, value, and potential impact if disclosed, altered, or destroyed. Classification levels include (but are not limited to):

Confidential – highly sensitive information requiring the strictest access controls.

Internal Use Only – non-public information intended for internal stakeholders.

Public – information approved for external distribution.

Each classification level determines the handling procedures for storage, transmission, access, and disposal.

All employees/contractors must handle information in accordance with its classification, using appropriate safeguards such as encryption, secure file transfer, access control, and secure destruction methods.

2.2. 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 password-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/contractors from a Company 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 the Company, unless posting is during business duties.

Employees/contractors must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

2.3. Unacceptable Use

The following activities are, in general, prohibited. Employees/contractors may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration 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 **the Company** authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing **Company**-owned resources.

The lists below are not exhaustive but provide a framework for unacceptable use:

2.4. System and Network Activities

Strictly prohibited activities include, but are not limited to:

- Violations of intellectual property laws, including the use or distribution of unlicensed software not authorized by **the Company**.
- Unauthorized copying of copyrighted materials such as photos, music, and software without valid licensing.
- Accessing data, servers, or accounts for purposes not related to **the Company's** business, even if access is otherwise authorized.
- Illegal exporting of software or technology in violation of export control laws.
- Introduction of malicious software such as viruses, ransomware, or worms into the network.
- Sharing passwords or allowing others (including family) to use **Company** accounts.
- Using **Company** resources to access or transmit content violating workplace conduct laws.
- Making fraudulent offers or unauthorized statements using **Company** accounts.
- Attempting to bypass or disrupt network security, including sniffing, spoofing, brute force attacks, or other forms of intrusion.
- Performing scans or monitoring unless explicitly authorized by the Infosec team.
- Circumventing user authentication or network security.
- Deploying honeypots or denial-of-service attacks.
- Sending disruptive scripts or messages to interfere with others' sessions.
- Sharing employee information with external parties without authorization.

2.4. Email and Communication Activities

When using **Company** resources to access the Internet, employees/contractors represent **the Company**. If stating affiliation, they must also clarify: "the opinions expressed are my own and not necessarily those of the Company."

Prohibited behaviors include:

- Sending unsolicited email or advertising (spam).
- Harassment through any communication method.
- Forgery of email headers or identity.
- Email solicitation to harass or harvest responses.
- Chain letters, Ponzi schemes, or mass unsolicited messages.
- Using **Company** infrastructure for external spam or advertising.

2.5 Blogging and Social Media

Blogging or posting on social media, even via personal devices, must comply with this Policy. Occasional and professional use of Company systems for such activity is acceptable only if it does not violate policies, affect productivity, or harm the Company's interests.

Employees/contractors must not:

Share Company confidential or proprietary information or trade secrets.

Make posts that harm the Company's image or violate anti-harassment policies.

Imply or state they represent the Company, unless authorized.

Use Company intellectual property (logos, trademarks) without permission.

Employees/contractors assume full responsibility for any content they publish.

2.6 Database

2.6.1. Secure Use of Database Credentials

In order to maintain the security of our internal databases, access by software programs should be granted only after proper authentication using valid credentials. These credentials are expected to be managed securely and should not reside in the main, executing body of the program's source code in clear text or in a form that can be easily reversed. It is also recommended that database credentials not be stored in any location accessible through a web server.

Encryption and authentication methods in use should follow widely accepted industry standards. The use of strong asymmetric encryption algorithms—such as RSA or elliptic-curve-based methods—is encouraged where applicable.

2.6.2. Storage of Database Usernames and Passwords

- Database usernames and passwords **should** be stored in a file separate from the program's core executable code. This file **should not** be readable or writeable by unauthorized users.
- Alternatively, database credentials **may** be located on the database server, with a hashed reference stored in the code.
- It is also acceptable to rely on an authentication service (such as a directory service) to handle database authentication on behalf of the program. In such cases, programmatic access to the credentials is unnecessary.
- Under no circumstances should credentials be stored in a web server's document tree.
- Passwords or passphrases used for database access **should follow** the Company's Password Policy.

2.6.3. Retrieval of Database Usernames and Passwords

- If credentials are stored in an external file (not embedded in source code), they **should** be read only at the moment of use. After successful authentication, any memory storing credentials **should be** promptly released or cleared.
- Credential storage **should be logically and physically separated** from the rest of the application code. Ideally, this means placing them in a dedicated file or module, containing only the credentials and strictly necessary functions or routines to retrieve them.
- In interpreted or script-based environments, it is strongly advised to avoid placing credential files in the same browsable or executable directory as the main application logic.

2.6.4. Access to Database Usernames and Passwords

Each application or functional program group is expected to use its own set of database credentials. Credential sharing between unrelated programs is discouraged.

Database passwords used by applications are to be treated with the same level of care as system-level passwords, as defined by our internal password handling policies.

Development teams should implement processes to ensure that credentials are:

- Regularly updated
- Accessible only on a strict need-to-know basis
- Managed in accordance with Company security standards

Any access to sensitive data, whether by users or software, should be limited to authorized functions. Privileged operations must be restricted to defined roles.

2.6.5. Secure Coding Practices

Developers are encouraged to follow secure coding guidelines appropriate to the programming languages and frameworks in use (e.g., Java, C, Python, scripting languages). The Company may provide or refer to internal best practices to support secure implementation of credential handling, access control, and secure storage mechanisms.

3. Configuration Management

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

- CFG-01 Maintain a library of approved operating system configuration benchmarks to ensure that each organization's operating systems are configured securely.
- CFG-02 Ensure that the organization's approved operating system configuration benchmark defines the organization as able to disable all unnecessary services in the operating system.
- CFG-03 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall define configuration benchmarks for each necessary service, including databases, SMB services, tiny services, VoIP, and similar services.
- CFG-04 Ensure that the organization's approved operating system configuration benchmark defines the organization as having unnecessary scripting languages in the operating system.
- CFG-05 Ensure that the organization's approved operating system configuration benchmark defines it as enabling advanced logging for operating system shells (such as Microsoft PowerShell or BASH).
- CFG-06 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall enforce cybersecurity services such as Data Execution Protection (DEP), Address Space Layout Randomization (ASLR), and User Account Control (UAC).
- CFG-07 Ensure that the organization's approved operating system configuration benchmark defines its ability to disable autorun on its operating system.
- CFG-08 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall enable machine locks (screensavers) after a defined period of inactivity.
- CFG-09 Ensure that the organization's approved operating system configuration benchmark defines the organization as requiring a secure boot process to verify the integrity of the operating system before loading (such as UEFI).
- CFG-10 Ensure that the organization's approved operating system configuration benchmark defines that the organization shall disable unnecessary wireless protocols and networks on the organization's endpoints.
- CFG-11 Maintain a library of approved software application configuration benchmarks that will be used to ensure that each of the organization's software applications is configured securely.
- CFG-12 Maintain a configuration enforcement system to enforce the organization's approved operating system and application configurations on each of the organization's computing systems.
- CFG-13 Ensure that the organization's configuration enforcement system enforces the organization's approved operating system and application configurations, regardless of the computing system's location (whether onsite or operating remotely).

4. Asset Management

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

CSP-01	Maintain an inventory of each of the organization's authorized Cloud Service Providers (CSPs).
CSP-02	Maintain an inventory of each service authorized for use in each authorized Cloud Service Provider (CSP).
CSP-03	Maintain an inventory of the organization's authorized Software-as-a-Service (SaaS) providers.
CSP-04	Maintain an inventory of the accounts authorized for use in each of the authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers.
CSP-05	Maintain a cybersecurity configuration benchmark for each of the organization's authorized Cloud Service Providers (CSPs).
CSP-06	Maintain a cybersecurity configuration benchmark for each of the services authorized for use in each of the organization's authorized Cloud Service Providers (CSPs).
CSP-07	Maintain a cybersecurity configuration benchmark for each of the organization's authorized Software-as-a-Service (SaaS) providers.
CSP-08	Maintain a cloud configuration vulnerability management system to regularly scan each of the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers for potential cybersecurity vulnerabilities.
CSP-09	Maintain a Data Loss Prevention (DLP) system to log and alert on potential data loss events in the organization's Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers regularly.
CSP-10	Ensure that appropriate logs from the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are enabled on the cloud platform.
CSP-11	Ensure that appropriate logs from the organization's authorized Cloud Service Providers (CSPs) or Software-as-a-Service (SaaS) providers are aggregated into the organization's log management system.

5. Email Management

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

EM-01	Maintain an inventory of each of the domain names authorized to use email.
EM-02	Maintain an inventory of Mail Transfer Agents (MTAs) authorized for each of the organization's approved email domains.
EM-03	Maintain appropriate Domain Name System (DNS) records for each of the organization's approved email domains (including SPF, DKIM, and DMARC).
EM-04	Ensure that the organization's email systems require encrypted connections (TLS) between all email servers, whether internal or external.
EM-05	Ensure that the organization's email systems block emails from domains that do not utilize the appropriate Domain Name System (DNS) records (including SPF, DKIM, and DMARC).
EM-06	Ensure that the organization's email systems perform spam content filtering for all emails (received by or sent by the organization).
EM-07	Ensure that the organization's email systems perform malware content filtering for all emails (received by or sent by the organization).
EM-08	Ensure that the organization's email systems perform anti-phishing content filtering for all emails (received or sent by the organization).

EM-09	Ensure that the organization's email systems perform anti-phishing URL filtering for all emails (received by or sent by the organization).
EM-10	Ensure that the organization's email systems filter data content for all of the organization's email (received by or sent by the organization).
EM-11	Ensure that the organization's email systems perform attachment filtering for all emails (received by or sent by the organization), including utilizing sandboxes to validate each attachment.
EM-12	Maintain a file transfer portal system that is separate from the organization's email system and that the organization can use to send large files to individuals outside of the organization.

6. Privileged Account Management

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

PAM-01	Maintain an inventory of all privileged accounts configured on endpoint computing systems.
PAM-02	Maintain an inventory of all privileged accounts configured on server computing systems.
PAM-03	Maintain an inventory of all privileged accounts configured on network devices.
PAM-04	Maintain an inventory of all privileged accounts configured on enterprise business applications.
PAM-05	Ensure all privileged accounts on endpoint computing systems are authorized and dedicated privileged accounts are required.
PAM-06	Ensure that all privileged accounts on server computing systems are authorized and require dedicated privileged accounts.
PAM-07	Ensure all privileged accounts on network devices are authorized and require dedicated privileged accounts.
PAM-08	Ensure that all privileged accounts on enterprise business applications are authorized and require dedicated privileged accounts.
PAM-09	Ensure that all default privileged accounts are not using their default system credentials to authenticate to the system.
PAM-10	Ensure that the organization does not allow shared privileged accounts for workforce members except in documented cases for emergency access or via a Privileged Account Management (PAM) system.
PAM-11	Maintain a Privileged Account Management (PAM) or Password Manager (PM) system for documenting service, shared accounts, or shared secrets between workforce members.
PAM-12	Maintain a Privileged Account Management (PAM) system to automatically rotate the credentials (using unique credentials) for each endpoint or server computing system.
PAM-13	Maintain a Privileged Account Management (PAM) system to automatically rotate the credentials (using unique credentials) for each network device.
PAM-14	Ensure the organization's Identity Providers (IDPs) require Multi-Factor Authentication (MFA) for all privileged accounts.

- PAM-15 Ensure the organization's Identity Providers (IDPs) logs and alerts when changes are made to privileged group memberships.
- PAM-16 Ensure the organization's Identity Providers (IDPs) log and alert account logon events (successful and failed) for all privileged accounts.

7. Program Management

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

- PRG-01 Maintain a cybersecurity program charter that authorizes the existence of a program and gives authority to the program team to use organizational resources to achieve the program objectives.
- PRG-02 Ensure that the organization's cybersecurity program charter defines its scope and applicability to each of the organization's business units or related entities.
- PRG-03 Ensure that the organization's cybersecurity program charter defines the ultimate goal of the cybersecurity program as the confidentiality, integrity, and availability of the organization's information systems.
- PRG-04 Ensure that the organization's cybersecurity program charter defines all the cybersecurity regulations and standards it shall use to define its goals for specific cybersecurity safeguards.
- PRG-05 Ensure that the organization's cybersecurity program charter or supporting documentation formally defines the organization's approach to cybersecurity governance and risk management.
- PRG-06 Ensure that the organization's cybersecurity program charter defines the executive leadership sponsor for the organization's cybersecurity program.
- PRG-07 Ensure that the organization's cybersecurity program charter establishes the authority of the stakeholder committee responsible for the program.
- PRG-08 Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific stakeholder committee members responsible for the organization's cybersecurity program.
- PRG-09 Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific members of the stakeholder committee responsible for its cybersecurity program and that they are from a diverse set of business units, not simply the technology teams.

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

- PRG-01 Maintain a cybersecurity program charter that authorizes the existence of a program and gives authority to the program team to use organizational resources to achieve the program objectives.
- PRG-02 Ensure that the organization's cybersecurity program charter defines its scope and applicability to each of the organization's business units or related entities.
- PRG-03 Ensure that the organization's cybersecurity program charter defines the ultimate goal of the cybersecurity program as the confidentiality, integrity, and availability of the organization's information systems.
- PRG-04 Ensure that the organization's cybersecurity program charter defines all the cybersecurity regulations and standards it shall use to define its goals for specific cybersecurity safeguards.

PRG-05	Ensure that the organization's cybersecurity program charter or supporting documentation formally defines the organization's approach to cybersecurity governance and risk management.
PRG-06	Ensure that the organization's cybersecurity program charter defines the executive leadership sponsor for the organization's cybersecurity program.
PRG-07	Ensure that the organization's cybersecurity program charter establishes the authority of the stakeholder committee responsible for the program.
PRG-08	Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific stakeholder committee members responsible for the organization's cybersecurity program.
PRG-09	Ensure that the organization's cybersecurity program charter or supporting documentation lists the specific members of the stakeholder committee responsible for its cybersecurity program and that they are from a diverse set of business units, not simply the technology teams.

8. Resilience Management

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

RES-01	Maintain a documented Business Continuity and Disaster Recovery (BCP / DR) program that documents the organization's safeguards to address business continuity.
RES-02	Maintain a documented cybersecurity Incident Management (IM) program that documents the organization's safeguards to address cybersecurity incident management.
RES-03	Ensure that the organization's documented Incident Management (IM) plan defines workforce members' roles and responsibilities during a cybersecurity incident.
RES-04	Ensure that the organization's documented Incident Management (IM) plan defines the leadership and decision-making responsibilities workforce members have during a cybersecurity incident.
RES-05	Ensure that the organization's documented Incident Management (IM) plan defines a communications plan the organization should use during a cybersecurity incident.
RES-06	Ensure that the organization's documented Incident Management (IM) plan defines how incidents should be reported to the organization (including how to handle whistleblowing cases).
RES-07	Ensure that the organization's documented Incident Management (IM) plan defines how to report to external groups (such as partners, law enforcement, regulators, and others) during a cybersecurity incident.
RES-08	Ensure that the organization's documented Incident Management (IM) plan defines how to report a cybersecurity incident to those impacted by the incident.
RES-09	Ensure that the organization's documented Incident Management (IM) plan defines the roles and responsibilities of the technical incident response team or security operations center during a cybersecurity incident.
RES-10	Ensure the organization's documented Incident Management (IM) plan defines how and where to document cybersecurity incidents.
RES-11	Ensure that the organization's documented Incident Management (IM) plan defines categories or classifications levels of cybersecurity incidents and how to classify incidents at each level.

RES-12	Ensure that the organization's documented Incident Management (IM) plan defines the requirement that the organization perform root cause analysis of each cybersecurity incident.
RES-13	Define a process the organization shall use to ensure that the organization's documented Incident Management (IM) plan defines how the documentation will be regularly reviewed and updated.
RES-14	Define a process for regularly testing the organization's Incident Management (IM) plans.
RES-15	Regularly perform tabletop exercises with key stakeholders to test the organization's Business Continuity and Disaster Recovery (BCP / DR) and Incident Management (IM) plans.
RES-16	Define a process the organization shall use to report Incident Management (IM) statistics to the organization's business stakeholders.
RES-17	Maintain technical cybersecurity tools to help the organization detect and respond to cybersecurity incidents as described in the organization's Incident Management (IM) plans.
RES-18	Regularly test the organization's cybersecurity Incident Management (IM) tools to ensure they function as expected to help it detect and respond to cybersecurity incidents.
RES-19	Maintain a cybersecurity forensics and threat-hunting program to help the organization detect and respond to cybersecurity incidents.
RES-20	Maintain cybersecurity forensics tools to help the organization create forensics images of computing systems to detect and respond to cybersecurity incidents.
RES-21	Define a process the organization shall use to update its Business Continuity and Disaster Recovery (BCP / DR) and Incident Management (IM) documentation after changes to its information technologies.
RES-22	Maintain an enterprise backup architecture to regularly create backups of the organization's computing systems and data.
RES-23	Maintain a trusted system image for each class of computing endpoint to ensure that it can be quickly restored in the case of a cybersecurity incident.
RES-24	Maintain a trusted system image for each computing server to ensure that it can be quickly restored in the case of a cybersecurity incident.
RES-25	Maintain technical access controls on each of the organization's backups to ensure that only authorized users have access to them (including encrypting physical access controls).
RES-26	Maintain immutable backups for each of the organization's computing systems and data to ensure they cannot be accidentally deleted or by malicious individuals.
RES-27	Define a process the organization shall use to test the organization's backups regularly.

9. Risk Communication Management

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

COM-01	Maintain a Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform to document, track, and report on the organization's cybersecurity risks.
--------	--

- COM-02 Ensure the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform maps its cybersecurity tools against approved and prioritized cybersecurity safeguards.
- COM-03 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform automatically integrates with all appropriate cybersecurity technologies to aggregate data regarding potential cybersecurity risks.
- COM-04 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform manually records the status of cybersecurity safeguards that cannot be automatically entered into the system.
- COM-05 Ensure the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform defines quality thresholds for each aggregated, quantified data point.
- COM-06 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes dashboards that report cybersecurity risk on a safeguard basis.
- COM-07 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes dashboards that report cybersecurity risk per business unit.
- COM-08 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform utilizes
dashboards that report cybersecurity risk in a way that takes approved exceptions into account and in a way that does not take approved exceptions into account.
- COM-09 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to executive leadership stakeholders.
- COM-10 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to business stakeholders.
- COM-11 Ensure that the organization's Governance, Risk, and Compliance (GRC) or similar cybersecurity business intelligence software platform regularly reports cybersecurity risk to technical stakeholders.

10. Safeguard Implementation Management

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

- IMP-01 Define a process the organization will use to document and track each of its cybersecurity projects (such as a formal Project Management Office (PMO)).
- IMP-02 Maintain a cybersecurity project tracking system (such as a Project Management Office (PMO) tool) to track each organization's cybersecurity projects.
- IMP-03 Ensure the organization's cybersecurity project tracking system is used to document each of the organization's active cybersecurity projects.
- IMP-04 Ensure the organization's cybersecurity project tracking system prioritizes each of its active cybersecurity projects.
- IMP-05 Ensure the organization's cybersecurity project tracking system is used to track the capital implementation costs for each organization's active cybersecurity project.

IMP-06	Ensure the organization's cybersecurity project tracking system is used to track the personnel implementation costs for each organization's active cybersecurity project.
IMP-07	Ensure the organization's cybersecurity project tracking system is used to track the status of each organization's active cybersecurity project.
IMP-08	Define a process the organization shall use to document and track each of the organization's approved cybersecurity exceptions when these cause information systems or software applications to be out of compliance with the organization's approved cybersecurity safeguards.
IMP-09	Define a process the organization shall use to document which business stakeholder(s) are authorized to approve cybersecurity exceptions in the organization's cybersecurity exception process.
IMP-10	Maintain a system to track all approved and documented cybersecurity exceptions to the organization's approved cybersecurity safeguards (such as a Governance, Risk, and Compliance (GRC) system or risk register).
IMP-11	Define a process the organization shall use to document and track each of the organization's issues (or defects) when these cause information systems or software applications to be out of compliance with the organization's approved cybersecurity safeguards.
IMP-12	Ensure that the organization assigns appropriate resources to address each of its cybersecurity projects and issues in a timely manner.
IMP-13	Regularly review each of the cybersecurity projects, cybersecurity exceptions, and cybersecurity issues to the organization's approved cybersecurity safeguards and report the status of each to the organization's leadership team.

11. Safeguard Selection Management

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

SAF-01	Maintain a detailed and documented taxonomy of all cybersecurity threats that could harm the organization's information systems.
SAF-02	Regularly evaluate cybersecurity threats to the organization and define, document, and approve cybersecurity safeguards to address these threats.
SAF-03	Maintain subscriptions to relevant cybersecurity threat intelligence feeds to ensure the organization's threat taxonomy is updated with the latest cybersecurity threats.
SAF-04	Maintain a detailed and documented list of characteristics that will be used to model each threat in the organization's cybersecurity threat taxonomy.
SAF-05	Ensure that the organization's threat model prioritizes each of the threats in the organization's cybersecurity threat taxonomy.
SAF-06	Maintain a documented board of directors-level cybersecurity policy that defines the high-level categories of cybersecurity safeguards that will be implemented to achieve the goals defined in the organization's cybersecurity program charter.
SAF-07	Maintain a detailed and documented list of all appropriate cybersecurity safeguards the organization must implement to achieve the goals defined in its cybersecurity program charter.
SAF-08	Ensure that the organization has aspirationally defined a complete list of the appropriate cybersecurity safeguards it must implement to achieve the goals defined in its cybersecurity program charter.

SAF-09	Ensure that the organization's cybersecurity safeguard documentation clearly defines the scope of applicability for each documented cybersecurity safeguard.
SAF-10	Ensure that the organization's cybersecurity safeguard documentation clearly defines the sanctions imposed if the documented cybersecurity safeguards are violated.
SAF-11	Ensure that the organization's cybersecurity safeguard documentation clearly defines mappings to regulatory or standards-based requirements for each documented cybersecurity safeguard.
SAF-12	Ensure that the organization's cybersecurity safeguard documentation clearly defines a business stakeholder responsible for each documented cybersecurity safeguard.
SAF-13	Ensure that the organization's cybersecurity safeguard documentation clearly defines the job roles that must be aware of each of the documented cybersecurity safeguards.
SAF-14	Ensure that the organization's cybersecurity safeguard documentation clearly defines a quantifiable measure of compliance for each of the documented cybersecurity safeguards.
SAF-15	Maintain detailed and documented acceptable use statements that define how an organization's workforce members shall appropriately utilize information systems.
SAF-16	Ensure that each prioritized threat in the organization's cybersecurity threat model is mapped against each of the corresponding cybersecurity safeguards in the organization's list of documented safeguards.
SAF-17	Regularly review all of the documentation used to define the organization's cybersecurity safeguards to ensure they are appropriate and up-to-date.

12. Safeguard Validation Management

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

VAL-01	Maintain a cybersecurity safeguard validation (audit) plan that documents the assessments the organization shall perform to validate the quality of the organization's cybersecurity safeguards.
VAL-02	Ensure that the organization's cybersecurity safeguard validation (audit) plan is a multi-year plan that regularly addresses all of the scopes the organization should assess.
VAL-03	Ensure that the organization's cybersecurity safeguard validation (audit) plan establishes criticality rankings for each of the assessment scopes in its assessment plan.
VAL-04	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines who should perform each assessment scope in its assessment plan.
VAL-05	Ensure that the organization's cybersecurity safeguard validation (audit) plan includes each of the cybersecurity penetration testing scopes it should assess regularly.
VAL-06	Ensure that the organization's cybersecurity safeguard validation (audit) plan includes software application penetration tests in its assessment plan.
VAL-07	Ensure that the organization's cybersecurity safeguard validation (audit) plan includes red team cybersecurity assessments in its assessment plan.
VAL-08	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines where cybersecurity penetration testing should be performed only against test systems due to the sensitivity of such systems.

VAL-09	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines how cybersecurity penetration testing should utilize vulnerability scanners as a part of the assessments.
VAL-10	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines when cybersecurity penetration testing should be documented in machine-readable formats (such as SCAP).
VAL-11	Ensure that the organization's cybersecurity safeguard validation (audit) plan defines how the organization will monitor user accounts during cybersecurity penetration tests.
VAL-12	Ensure that the organization's leadership stakeholders regularly approve the organization's cybersecurity safeguard validation (audit) plan.
VAL-13	Ensure that the organization's leadership stakeholders regularly allocate and assign resources to the organization's safeguard validation (audit) plan and complete each assessment according to the schedule defined.
VAL-14	Ensure that the organization documents the results of each cybersecurity assessment in a central software platform (such as a Governance, Risk, and Compliance (GRC) tool).
VAL-15	Ensure that the organization tracks the progress of each cybersecurity assessment in a central software platform (such as a Governance, Risk, and Compliance (GRC) tool).
VAL-16	Ensure that the organization regularly reports the results of each cybersecurity assessment to its leadership stakeholders.

13. Software Management

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

SW-01	Maintain a system to maintain an inventory of the organization's approved software.
SW-02	Ensure the organization's software inventory system records appropriate demographics for each software application.
SW-03	Ensure the organization's software inventory system regularly updates the software inventory via an automated discovery tool.
SW-04	Ensure the organization's software inventory system correlates the organization's hardware and software inventories in the same system.
SW-05	Ensure the organization's software inventory system validates that all software in the inventory is still supported by the software vendor.
SW-06	Ensure the organization's software inventory system validates that all operating system software in the organization's software inventory is kept up to date.
SW-07	Ensure the organization's software inventory system validates that all application software in the organization's software inventory is kept up to date.
SW-08	Maintain a Service Level Agreement (SLA) for the organization to define how often software updates must be performed on each software application.
SW-09	Define a process the organization shall use to ensure all software adheres to the organization's approved software-update Service Level Agreement (SLA).
SW-10	Maintain a software application control system on each organization's computing systems to ensure that only authorized software can execute.

SW-11	Ensure the organization's application control system only allows the execution of authorized binaries on each of the organization's computing systems.
SW-12	Ensure the organization's application control system only allows authorized software libraries (such as DLLs) on each of the organization's computing systems.
SW-13	Ensure the organization's application control system only allows the use of authorized software scripts on each of the organization's computing systems.
SW-14	Ensure the organization's application control system only allows the use of authorized operating system shells (such as Microsoft PowerShell or BASH) on each of its computing systems.
SW-15	Define a process the organization shall use to remove unauthorized software from each of its computing systems in a timely manner.

14. 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 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.

15. Compliance and Legal Obligations

The Company is committed to full compliance with all applicable information security laws, regulations, and industry standards relevant to its operations and jurisdictions in which it conducts business. This includes, but is not limited to, data protection legislation (such as the General Data Protection Regulation (GDPR)), cybersecurity directives, financial services regulations, and sector-specific compliance requirements.

To this end, the Company ensures that:

- **Policies and procedures** are aligned with applicable legal and regulatory frameworks and are regularly reviewed and updated to reflect changes in legislation or industry best practices.
- **Technical and organizational measures** are implemented to safeguard the confidentiality, integrity, and availability of information assets in accordance with recognized standards such as ISO/IEC 27001, NIST, or equivalent frameworks.
- **Data processing and handling** activities are conducted lawfully, fairly, and transparently, with appropriate safeguards for personal and sensitive information.
- **Third-party engagements**, including outsourcing and vendor management, are governed by contractual and regulatory requirements, ensuring that external partners adhere to the same security and compliance standards as the Company.
- **Audit and monitoring mechanisms** are in place to assess compliance, detect violations, and enforce corrective actions where necessary.

All employees, contractors, and third parties subject to this Policy are required to understand and comply with the applicable legal and regulatory obligations as they relate to their role. Failure to comply may result in disciplinary action, up to and including termination of employment or contract, as well as potential legal consequences.

The Company promotes a culture of accountability and legal awareness, providing regular training and guidance to ensure that all personnel are informed of their responsibilities and the importance of maintaining regulatory compliance in all aspects of information security.

16. Security Awareness and Training

The Company recognizes that a well-informed workforce is essential to maintaining a strong security posture. To that end, all employees, contractors, and other individuals with access to the Company's information systems or data are required to participate in ongoing information security awareness and training programs.

The objectives of the security awareness and training program are to:

- **Educate personnel** about current and emerging cybersecurity threats, including phishing, social engineering, malware, insider threats, and other relevant risks.
- **Promote best practices** for secure behavior, including proper password management, secure handling of sensitive information, use of authorized devices, and safe internet practices.
- **Ensure understanding** of the Company's information security policies, procedures, and responsibilities, including how to report incidents or suspected breaches.
- **Reinforce a security-first culture**, encouraging vigilance, accountability, and proactive engagement in protecting the Company's assets and data.

Key components of the program include:

- **Mandatory training upon onboarding**, ensuring that new hires and contractors understand their security responsibilities from the outset.
- **Periodic refresher training**, conducted at least annually, with updates based on changes in the threat landscape, company policies, or regulatory requirements.
- **Targeted training**, as needed, for specific roles with elevated access or responsibilities (e.g., system administrators, developers, or incident responders).
- **Simulated exercises and awareness campaigns**, such as phishing simulations, posters, newsletters, and internal communications, to reinforce learning in practical contexts.

Participation in required training is tracked and monitored. Non-compliance may result in corrective measures, including access restrictions or disciplinary action. The Company continuously reviews and enhances its training materials to ensure they remain effective, relevant, and aligned with industry standards and regulatory expectations.

Through regular education and awareness, the Company aims to reduce human-related risk and empower personnel to act as the first line of defense against cyber threats.