**INFORMATION SECURITY POLICY**

**PURPOSE**

This policy establishes a framework for balancing robust information security measures with [EMPLOYER’S NAME]'s operational needs. It ensures compliance with legal requirements and aligns with the expectations of [customers/clients]. [EMPLOYER’S NAME] may apply varying levels of security controls to different information assets based on their risk level and other factors.

All members of [EMPLOYER’S NAME]’s workforce are required to review, understand, and adhere to this policy. While this document provides key guidance, it cannot address every potential security challenge. If you encounter situations that may introduce information security risks or require deviation from this policy, you must consult with your manager or a designated [EMPLOYER’S NAME]’s representative. Failure to seek or follow such guidance may be treated as a breach of this policy.

This policy is classified as confidential information. It must not be shared outside [EMPLOYER’S NAME] without express authorization from the Information Security Coordinator. However, it may be shared with approved contractors or vendors under a valid non-disclosure agreement or a similar confidentiality arrangement.

The trust of our [customers/clients], employees, and partners depends on our ability to safeguard their data. A cybersecurity breach can undermine our credibility, cause significant financial losses, and harm [EMPLOYER’S NAME]'s reputation. Maintaining a strong security posture requires commitment and vigilance from all individuals who handle or access our information assets, including employees, contractors, volunteers, and other authorized users. Information security is a shared responsibility.

This policy complies with all applicable state and Vermont laws.

Core principles

[EMPLOYER'S NAME] adheres to the following principles in the development and enforcement of information security controls:

1. Safeguarding the confidentiality, integrity, and availability of [EMPLOYER’S NAME]'s information assets [and those of its [customers/clients]].
2. Ensuring compliance with applicable laws governing information security, privacy, and data protection.
3. Balancing operational efficiency with the necessity of mitigating risks to sensitive, proprietary, or confidential information.
4. Limiting access to sensitive or confidential data based on a need-to-know basis and assigning the minimum level of access privileges required for job responsibilities.
5. Provide security training and resources to all workforce members, fostering awareness and empowering them to fulfill their information security obligations effectively.

**SCOPE**

This policy applies [across the entire [EMPLOYER'S NAME] enterprise/[APPLICABLE SCOPE]]. It provides specific information security guidance that must be followed alongside any obligations outlined in the [CODE OF CONDUCT OR EMPLOYEE HANDBOOK].

This document outlines [EMPLOYER'S NAME]'s overarching information security policy. In many cases, you are personally responsible for taking or avoiding specific actions as described. In other instances, the Information Security Coordinator, [IT/[IT ORGANIZATION NAME]], or another designated [EMPLOYER'S NAME] team member will take or refrain from such actions as required.

At times, [EMPLOYER'S NAME] may implement and distribute more detailed policies, procedures, standards, or processes tailored to specific locations, business units, or information security challenges. These additional materials are considered extensions of this policy. You must adhere to them when applicable unless you have received explicit approval for an exception.

**GUIDANCE**

No single policy can anticipate every information security issue you might encounter. Striking the right balance between protecting [EMPLOYER'S NAME]'s information assets and maintaining workflow efficiency can be challenging. A variety of administrative, physical, and technical safeguards are available, and their implementation may be simpler than assumed. Always seek assistance when in doubt.

Before engaging in any actions that could pose information security risks, you are required to seek guidance. Contact your manager for direction.

For questions related to this policy or technical security matters, reach out to: [INFORMATION SECURITY COORDINATOR CONTACT].

For inquiries regarding legal obligations[, including [customer/client] agreements], contact: [LEGAL CONTACT].

For additional detailed policies, procedures, standards, and processes, refer to [the Appendix/[INTERNAL WEBSITE OR OTHER MAINTAINED LISTING]].

**PRIVACY AND MONITORING EXPECTATIONS**

Unless otherwise required by applicable law, you should not expect privacy when using [EMPLOYER'S NAME]'s networks or systems. This includes activities such as transmitting and storing files, data, or messages.

To ensure compliance with [EMPLOYER'S NAME]'s policies and safeguard its interests, [EMPLOYER'S NAME] retains the right to monitor any use of its systems and networks, as permitted by applicable law. By accessing or using [EMPLOYER'S NAME]'s systems, you consent to such monitoring. Monitoring activities may include, but are not limited to:

* Reviewing network traffic, emails, and other messages or data transmitted or received.
* Examining data stored in file directories, hard drives, or other physical or digital media.

Compliance with regulatory standards

Various laws, regulations, and industry standards govern [EMPLOYER'S NAME]'s information security practices and the data it manages. [EMPLOYER'S NAME] is fully committed to adhering to these requirements, as they reflect both legal obligations and the trust placed in us by our [customers/clients].

This section outlines some of the most commonly encountered obligations. However, these are not exhaustive, and additional laws may apply. If you are collecting, creating, or handling new or unfamiliar types of data, consult [INSERT ROLE/DEPARTMENT] to clarify your responsibilities.

Protection of personal information and breach notification

Numerous laws safeguard personal information, including government-issued identifiers, financial account details, and other sensitive data. Many jurisdictions also require organizations to notify affected individuals in the event of a data breach involving personal information. In some regions, data protection laws mandate reasonable security measures or specific protections for personal data. These laws may apply to data relating to [EMPLOYER'S NAME]'s employees, [customers/clients], business partners, and other individuals.

Before collecting, generating, or using personal information, [contact [CONTACT NAME]/review [RESOURCE]].

Compliance with additional legal requirements

[Insert a list of other relevant laws, regulations, or standards here, along with brief descriptions and contact details for further guidance or resources.]

**RESPONSIBILITIES**

[EMPLOYER'S NAME] and its leadership are committed to establishing and maintaining a robust information security program.

Information security coordinator

[EMPLOYER'S NAME] has appointed [[TITLE]/[TITLE AND CONTACT]] as the Information Security Coordinator, responsible for overseeing all aspects of the organization's information security program. Any references to the Information Security Coordinator within this policy include both the designated individual and any authorized delegates acting on their behalf.

Policy authority and maintenance

[EMPLOYER'S NAME] has authorized the Information Security Coordinator to develop, update, and enforce this policy, as well as any supplementary policies, procedures, standards, or processes deemed necessary and appropriate.

Policy review

At least once per year, the Information Security Coordinator will conduct a review of this policy. This process will include input from relevant stakeholders, such as individual business units, [Human Resources/[SPECIFIC HR ORGANIZATION NAME]], Legal, and other applicable departments within [EMPLOYER'S NAME].

Exceptions

[EMPLOYER'S NAME] acknowledges that certain business needs or local circumstances may occasionally require an exception to this policy. All exception requests must be submitted [in writing/using [ONLINE OR OTHER PROCESS]]. The Information Security Coordinator is responsible for approving, documenting, and periodically reviewing all approved exceptions.

Approval of a similar exception in the past does not guarantee future approval. Each exception request will be evaluated based on the specific circumstances and potential risks to [EMPLOYER'S NAME]'s information assets [and those of our [customers/clients]].

To submit an exception request, [contact [CONTACT NAME]/follow the instructions provided in [RESOURCE]].

Workforce obligation to comply

All employees and contractors are required to adhere to the portions of this policy that apply to them. [This policy does not restrict any communications or actions that are protected or required under applicable law.]

[EMPLOYER'S NAME] considers any attempt to bypass or undermine security controls a violation of this policy. Prohibited actions include, but are not limited to:

* Sharing access credentials, such as passwords.
* Disabling or deactivating anti-malware software.
* Altering or removing secure system configurations.
* Establishing unauthorized network connections.

Exceptions to these rules may only be granted by the Information Security Coordinator, following the process outlined in the section titled *Exceptions* above.

**UNDERSTANDING AND REPORTING OBLIGATIONS**

[EMPLOYER'S NAME] provides resources to help employees and contractors understand this policy. However, you are ultimately responsible for your actions and for complying with this policy. If you encounter a situation that appears to violate this policy or poses undue information security risks, you must report it to your manager or the Information Security Coordinator.

Sanctions

Violations of this policy may result in disciplinary action or other penalties. Possible sanctions include suspension, access restrictions, reassignment of duties, or, in severe cases, termination of employment, consistent with applicable law. If [EMPLOYER'S NAME] suspects illegal activity, it reserves the right to report such actions to the appropriate authorities and cooperate fully with any investigations or prosecutions.

**TRAINING**

[EMPLOYER'S NAME] understands that a knowledgeable and vigilant workforce is the most effective defense against security threats. To this end, we provide security training opportunities and expert resources to help employees and contractors understand their responsibilities under this policy and mitigate risks.

Employees must complete information security training within [a reasonable period/[SET TIMEFRAME]] after their start date.

All workforce members are required to participate in annual information security training. Managers are responsible for ensuring their team members complete all mandated training.

Failure to complete required training may be considered a violation of this policy. [EMPLOYER'S NAME] will maintain attendance records and copies of the training materials provided.

Handling [customer/client] information

[EMPLOYER'S NAME] may manage sensitive [customer/client] information. In some cases, we may agree to adhere to specific [customer/client] information security policies or standards. To streamline operations, this policy is designed to address the common requirements shared by most [customers/clients].

If [EMPLOYER'S NAME] agrees to additional [customer/client]-specific security policies or standards, affected workforce members will be informed. Compliance with these policies or standards is mandatory, including participation in any related training or background screening requirements.

All [customer/client] agreements that impose specific information security obligations must be reviewed and approved by both Legal and the Information Security Coordinator.

**DATA CLASSIFICATION AND RISK CONTROLS**

[EMPLOYER'S NAME] employs a three-tier classification system to protect information based on its sensitivity and associated risk levels. This system enables [EMPLOYER'S NAME] to implement appropriate security controls while balancing protection, cost, and operational efficiency.

All information managed by [EMPLOYER'S NAME] is categorized into the following levels, listed from least to most sensitive:

1. Public information.
2. Confidential information.
3. Highly confidential information.

Unless explicitly marked as public information or clearly intended for public access, treat all [EMPLOYER'S NAME] [and [customer/client]] information as at least confidential information. This applies regardless of its format—whether digital, physical, verbal, or otherwise.

You are required to apply security controls that correspond to the classification level of the information you store, transmit, or handle. When feasible, use classification labels to ensure clarity.

Public information

Public Information is data that [EMPLOYER'S NAME] has intentionally made available to the general public. Information provided by another party (including [customers/clients]) that is subject to a current, signed non-disclosure agreement must never be classified or treated as public information.

Examples of public information include, but are not limited to:

* Press releases.
* Marketing materials created by [EMPLOYER'S NAME].
* Job postings or announcements.
* Any content published on [EMPLOYER'S NAME]'s publicly accessible website[s].

It is essential not to assume that information obtained from [EMPLOYER'S NAME]'s internal systems or networks is publicly available. For instance, draft versions of marketing materials are typically considered confidential information until officially released. Unless verified as public information, treat all information as at least confidential information, and ensure it is not disclosed without appropriate authorization.

Confidential information

Confidential information is data that, if improperly disclosed, could harm [EMPLOYER'S NAME], its [customers/clients], employees, or other entities or individuals. Such harm may include privacy violations, impacts on market competitiveness, or legal and regulatory liabilities. Confidential Information also includes information that is not otherwise publicly accessible.

When feasible, mark confidential information to indicate its status. Applications and databases containing confidential information may display an initial banner upon system access to reinforce its classification.

You must obtain authorization before disclosing confidential information to external parties. Consult with your manager or Legal to verify that a proper non-disclosure or other agreement is in place before sharing such information.

Confidential information includes, but is not limited to:

1. [EMPLOYER'S NAME]'s financial data, [customer/client] lists, revenue forecasts, project plans, and intellectual property.
2. Data, information, and intellectual property provided by [customers/clients].
3. Contracts with [customers/clients] and other external parties, including vendors.
4. Communications or records about internal [EMPLOYER'S NAME] matters, operations, or audits.
5. Policies, procedures, standards, and processes (e.g., this policy, which must not be shared without authorization).
6. Information labeled "confidential" or similarly classified by external parties under valid agreements.
7. Employee-related information.
8. Summaries, reports, or documents containing confidential information.
9. Drafts or working versions of any of the above.

You must protect confidential information by implementing administrative, physical, and technical safeguards appropriate to the risks involved. These include:

1. Authentication: Ensure online access to confidential information requires login credentials for [EMPLOYER'S NAME]'s network or approved services.
2. Discussions: Discuss confidential information only in non-public areas. If a public discussion is unavoidable, take steps to prevent being overheard.
3. Copying, printing, and scanning: Limit scanning, copying, or distributing confidential information to what is necessary and permitted under applicable agreements. Ensure unauthorized individuals cannot view the information.
4. [When faxing, include a cover sheet identifying the information as confidential. Use fax machines configured to confirm transmissions and store them in secure locations.]
5. Encryption: Encrypt confidential information stored on mobile devices such as laptops and smartphones. Consider encryption when transmitting or transporting data externally, based on the risk level. Contact your manager or [INFORMATION SECURITY COORDINATOR CONTACT] for assistance.
6. Mailing: For external distribution, use services requiring a recipient's signature. Internally, use sealed security envelopes marked "confidential information."
7. Meeting rooms: Share confidential information only in secure meeting rooms. Erase or remove such information from whiteboards or presentation tools after the meeting concludes.
8. Need to know: Access, share, or include confidential information only when there is a business need to know.
9. Physical security: Store systems or paper records containing confidential information in secured physical locations.

Highly confidential information

Highly confidential information is a subset of confidential information that requires enhanced protection due to the severe and potentially irreparable harm its unauthorized disclosure or misuse could cause to [EMPLOYER'S NAME], its [customers/clients], employees, or other parties.

Where feasible, mark highly confidential information to indicate its sensitivity. Applications or databases containing highly confidential information should display an initial banner upon access. Such information must not be removed from [EMPLOYER'S NAME]'s environment without explicit authorization.

Disclosing highly confidential information to external parties requires prior approval. Consult the Information Security Coordinator to ensure compliance with legal and contractual obligations before sharing this type of information.

Examples include, but are not limited to:

1. Personal information related to employees, [customers/clients], business partners, or others.
2. Sensitive business data such as budgets, financial results, or strategic plans.

To mitigate risks and comply with laws, regulations, and standards, highly confidential information must be protected through robust administrative, physical, and technical safeguards, including:

1. Authentication: Access to highly confidential information must require logging in to [EMPLOYER'S NAME]'s network or approved services and specific authorization.
2. Discussions: Discuss highly confidential information only in secure, non-public locations.
3. Copying, printing, and scanning: Avoid scanning, copying, or distributing highly confidential information unless absolutely necessary. Prevent unauthorized viewing by others without a specific business need.
4. [When faxing, include a cover sheet identifying the information as highly confidential and configure fax machines to confirm transmissions securely.]
5. Encryption: Encrypt highly confidential information when storing it on laptops, smartphones, or other mobile or stationary devices (e.g., USB drives or servers). Encryption is also mandatory when transmitting the data internally or externally.
6. Mailing: Avoid mailing highly confidential information unless absolutely necessary. For external mailing, use services requiring recipient signatures. Internally, use sealed envelopes marked " highly confidential information." If transmitted via online media, encrypt the data and require authentication for access.
7. Meeting rooms: Share highly confidential information only in physically secured meeting rooms. Erase or remove any displayed information (e.g., on whiteboards or presentation tools) after the meeting.
8. Need to Know: Access, share, or include highly confidential information only when there is a specific business need to know.
9. Network segmentation: Restrict access to highly confidential information to specific network areas based on business needs. Use segmentation controls such as firewalls or access control lists to isolate this data from other parts of [EMPLOYER'S NAME]'s network.
10. Physical security: Store highly confidential information in physically secured areas, accessible only to authorized personnel with a specific business need to know.

**ROLES, ACCESS CONTROLS AND ACCEPTABLE USE**

People play a critical role in information security, serving as both the strongest defense and the weakest link. [EMPLOYER'S NAME] grants access to systems and data based on defined business roles, placing restrictions on how information assets can be used. These measures are designed to minimize risks and protect both you and [EMPLOYER'S NAME].

Roles

Access to systems and data is determined by an individual's role within [EMPLOYER'S NAME] and the activities assigned to them.

*Employees*

[Human Resources/[SPECIFIC HR ORGANIZATION NAME]] oversees employee screening [and background checks]. Additional background screening or testing may be required for employees handling highly confidential information, where permitted by applicable laws. For more details, refer to [HR PROCESSES].

Supervising managers may only request access for employees to systems and data necessary to perform their business functions.

*External parties*

[EMPLOYER'S NAME] provides system access to approved external parties, including contractors, vendors, service providers, business partners, or others with a legitimate business need that cannot be met through alternative means. Access levels may vary based on specific business circumstances.

[A sponsoring employee must be assigned to any external party before access to [EMPLOYER'S NAME]'s systems or data is granted. The sponsoring employee is responsible for:

* Supervising the external party’s activities to ensure compliance with this policy.
* Requesting access only to resources necessary for the external party's business needs.
* Ensuring that any access granted is terminated promptly when the business need ends.]

**IDENTITY AND ACCESS MANAGEMENT**

[EMPLOYER'S NAME] employs identity and access management controls to assign appropriate privileges to employees and other users. Each individual is assigned a unique identifier, referred to as their "primary ID," created using a standardized algorithm. Device- or application-specific identifiers should only be created when the primary ID cannot be used, and these must be linked to an accountable individual.

Unique user accounts

Each individual is provided with a unique user account, password, and other authentication credentials tied to their primary ID. Sharing your account, password, or other credentials is strictly prohibited. If individual assignment of system or administrative accounts is not possible, mediated access, audit logs, or similar technical measures must be implemented to ensure accountability.

Adding, modifying or terminating access

Access to resources is restricted to individuals with a business need to know. Responsible managers [and sponsoring employees] must direct requests for adding or changing access to [IT/[IT ORGANIZATION NAME]].

System and application administrators are required to periodically review user accounts and access levels to ensure access remains justified.

When an employee leaves the organization, [Human Resources/[SPECIFIC HR ORGANIZATION NAME]] must immediately notify [IT/[IT ORGANIZATION NAME]] to ensure timely deactivation of the individual's accounts.

For external parties, the sponsoring employee must notify [IT/[IT ORGANIZATION NAME]] when access is no longer required.

Managers must consult [Human Resources/[SPECIFIC HR ORGANIZATION NAME]] and the Information Security Coordinator for guidance on access for employees on extended leave.

Authorization levels and least privilege

[EMPLOYER'S NAME] follows the principle of least privilege to ensure individuals only have the access necessary to perform their tasks. This applies to both user and administrative access. Administrative privileges must only be granted when there is a specific business need, and these should be limited to the extent feasible.

Role-based access controls

Role-based access controls should be used wherever possible to assign access based on business functions rather than on an individual basis. This approach supports least privilege, standardizes access, and simplifies periodic access reviews.

Acceptable use policy

[EMPLOYER'S NAME] provides network resources and systems to employees and other authorized individuals to support business operations. The use of these resources is subject to specific restrictions to protect [EMPLOYER'S NAME]'s information assets.

If you have questions about acceptable use, consult your manager or contact the Information Security Coordinator for guidance.

**GENERAL USE OF INFORMATION TECHNOLOGY RESOURCES**

[EMPLOYER'S NAME] provides network resources and systems to support business operations. Incidental personal use of these resources is permitted, provided it is limited to personal purposes and does not conflict with business interests. You must not use [EMPLOYER'S NAME]'s resources for commercial activities, personal gain, or actions that may create a real or perceived conflict of interest.

Do not engage in activities that negatively affect your job performance or interfere with others' ability to perform their duties. [EMPLOYER'S NAME]'s network and systems are subject to monitoring.

You are prohibited from using [EMPLOYER'S NAME]'s network or systems for any illegal activities. Suspected illegal actions may be reported to the authorities, and [EMPLOYER'S NAME] may cooperate in investigations or prosecutions.

Prohibited activities

The following activities are prohibited when using [EMPLOYER'S NAME]'s resources:

1. Accessing, uploading, downloading, or disseminating content or services that violate the law or [EMPLOYER'S NAME]'s policies on harassment, discrimination, or specific technologies.
2. Hacking, spoofing, or conducting denial-of-service attacks.
3. Gaining or attempting unauthorized access to networks or systems.
4. Sending fraudulent email messages.
5. Distributing or attempting to distribute malware.
6. Spying or installing unauthorized monitoring tools.
7. Engaging in criminal acts, such as fraud, terrorism, or identity theft.
8. Downloading, storing, or distributing obscene materials or child pornography.
9. Downloading or sharing copyrighted materials without authorization.
10. Creating security risks or degrading system performance.
11. Causing harm to [EMPLOYER'S NAME] through embarrassment, reputational damage, or other means.
12. Sending spam, chain letters, hoax emails, or commercial solicitations.
13. Disrupting the workplace or creating a hostile environment.
14. Using encryption or similar methods to conceal inappropriate activities.
15. Installing or using unlicensed or pirated software.

Desktop, laptop and end-user controls

Access to [EMPLOYER'S NAME]'s network is permitted only via approved end-user devices that meet the organization's current security standards. These standards may include requirements such as anti-malware software, system patches, and specific software versions. [EMPLOYER'S NAME]-owned devices may be configured for automatic upgrades. Remote access may be denied for personal devices that fail to meet these standards.

Use only your assigned [EMPLOYER'S NAME] account(s) to access its systems unless explicitly authorized to use an alternative or administrative account.

To protect confidential information, activate a locking screen saver after a maximum of [15/[TIME LIMIT]] minutes of inactivity. If you handle highly confidential information, lock your screen whenever it is left unattended.

**INFORMATION HANDLING AND STORAGE**

You are required to handle, store, and securely dispose of [EMPLOYER'S NAME]'s information in compliance with the [Records Retention Schedule/[RECORDS POLICY NAME]]. You are responsible for safeguarding any confidential or highly confidential information you access or store. Do not permit unauthorized individuals to view, access, or use such information unless they have a specific business need to know.

Storage requirements

* Business critical data: Store all files or data essential to [EMPLOYER'S NAME]'s operations on regularly maintained and backed-up servers or other approved storage systems. Do not store business-critical information solely on end-user devices, such as desktops, laptops, smartphones, or other mobile devices.
* Physical media security: Secure all media containing [EMPLOYER'S NAME]'s information—such as hard drives, CDs, paper records, removable drives (e.g., USB drives), or voice recordings—in a locked area when not in use.

Disposal requirements

* Paper disposal: Shred or otherwise destroy any paper documents containing confidential or highly confidential information before discarding them.
* Online media disposal: Return all media containing [EMPLOYER'S NAME]'s information, including hard drives and removable storage devices, to [IT/[IT ORGANIZATION NAME]] for secure disposal when it is no longer needed for business purposes.

**INTERNET USE**

The internet provides essential services that enable [EMPLOYER'S NAME]'s employees and contractors to work effectively. However, some technologies pose risks to [EMPLOYER'S NAME]'s assets, and certain uses are inappropriate in the workplace. Access to specific services, websites, or internet-based functions may be blocked or restricted based on risk assessments and business needs. You must not access inappropriate or offensive websites using [EMPLOYER'S NAME]'s resources.

General internet use

Limit web browsing, streaming media (e.g., videos, audio streams, webcasts), and other internet services to business-related purposes, unless otherwise permitted by this policy. Internet usage must align with this policy.

* Peer-to-peer file sharing: Do not use peer-to-peer file sharing services without explicit, documented approval from the Information Security Coordinator due to the risks they pose to information assets.
* Remote access services: Do not use internet-based remote access tools to connect to [EMPLOYER'S NAME]'s network or systems, including desktop computers. For remote access, only use methods provided or authorized by [EMPLOYER'S NAME].

Email and social media

Confidential or highly confidential information must not be disclosed on blogs, social media, unsecured emails, or chat messages (see ROLES, ACCESS CONTROLS AND ACCEPTABLE USE). Only authorized individuals may post or send messages that represent [EMPLOYER'S NAME].

* Professional communication: Draft and send communications with professional judgment, recognizing that messages may be forwarded outside your control. Email signatures should be appropriate, professional, and concise.
	+ Email footer: Use [EMPLOYER'S NAME]'s standard footer on all external emails. Do not alter or omit it.
* Attachments and links: Avoid opening unexpected email attachments or clicking unfamiliar links, as these are common methods for malware delivery. Even familiar-looking messages may be falsified (spoofed).
* Responding to requests for information: Verify the sender’s identity and purpose before responding to any message requesting confidential or highly confidential information.
* Suspicious messages: Contact [IT/[IT ORGANIZATION NAME]] immediately if you suspect a message is malicious. Do not interact with suspicious content, including clicking unsubscribe links.

Cloud computing

Cloud computing services, which store data and provide services via internet-accessible data centers, are used by [EMPLOYER'S NAME] based on business needs. These services can introduce risks, including legal compliance challenges and varying security measures.

Before using any cloud computing service to collect, create, store, or manage [EMPLOYER'S NAME]'s confidential or highly confidential information, obtain approval from Legal and the Information Security Coordinator.

This policy applies to all document-sharing and internet-based services involving [EMPLOYER'S NAME]'s confidential or highly confidential information.

**MOBILE DEVICES AND BRING YOUR OWN DEVICE POLICY**

Mobile devices, including laptops, smartphones, and tablets, enhance productivity and support business needs. However, these devices also introduce risks to [EMPLOYER'S NAME]'s information assets. To mitigate these risks, employees and others must take necessary precautions to protect mobile devices and any data stored on them.

Personal devices

[EMPLOYER'S NAME] may allow employees and authorized individuals to use their personal devices to access its network and systems. By choosing to do so, you agree to comply with this policy and any additional policies, procedures, or standards [EMPLOYER'S NAME] enforces.

You may be required to install specific security measures on your device, such as device management software, access controls, encryption, or remote wiping capabilities in case of loss or theft.

[IT/[IT ORGANIZATION NAME]] or an authorized representative may review your device and remove [EMPLOYER'S NAME] data if you leave the organization, change devices or services, or in similar scenarios.

You must provide access to your device promptly upon request for legitimate business purposes, including security incidents or investigations.

Data protection and device security

All mobile devices containing [EMPLOYER'S NAME]'s confidential or highly confidential information must be protected using encryption and approved security measures, such as device management software or access controls. Devices with access to [EMPLOYER'S NAME] email accounts must also use an approved authentication method.

* Physical security:
	+ Secure mobile devices physically when not in use.
	+ Never leave laptops or devices unattended unless locked or otherwise secured.
	+ Avoid leaving devices or their carrying bags visible in parked cars, and do not check devices as luggage on airlines or other public transport.
* Network security:
* Do not connect mobile devices containing [EMPLOYER'S NAME] information to unsecured networks unless they are protected by an up-to-date firewall or similar security measures.
* Unsecured networks include home Wi-Fi, hotel networks, open wireless hotspots, conference networks, or any network not approved or controlled by [EMPLOYER'S NAME].

Additional requirements

If your device contains confidential or highly confidential information, you must use security strategies, such as remote wiping, to protect it from unauthorized access in case of loss or theft. Always follow [EMPLOYER'S NAME]'s standards for mobile device usage to safeguard information assets.

**REMOTE ACCESS**

If you need to access [EMPLOYER'S NAME]'s network and systems remotely (e.g., from home, while traveling, or at another location), remote access may be granted based on business needs.

* Authentication and authorization: Use multifactor authentication for remote access. Access should be limited to only the assets and functions approved by the Information Security Coordinator.
* Approved methods: Remote access must be conducted using [EMPLOYER'S NAME]-provided and authorized methods, such as an approved VPN, secure network connection, or designated portal. Do not install or configure any other remote connections, including remote desktop software, without explicit authorization.
* Timeouts and split tunneling: Remote access connections must timeout after [one hour/[TIME LIMIT]] of inactivity. Split tunneling or other mechanisms that connect unsecure networks with [EMPLOYER'S NAME]'s network are prohibited.

External network connections

In specific business situations (e.g., collaborating with [customers/clients], outsourcing, or partnerships), a secure extranet connection between [EMPLOYER'S NAME]'s network and an external party's network may be necessary.

The Information Security Coordinator must review and approve all external connections, including extranets. Approval requires a valid business agreement between the parties. Extranet connections must be limited to the resources necessary for the specified functions. [EMPLOYER'S NAME] monitors these connections and may deactivate them if unusual or inappropriate activity is detected.

Wireless network connections

Wireless access points (WAPs), routers, or similar devices may not be connected to [EMPLOYER'S NAME]'s network without prior review and approval by the Information Security Coordinator.

* Security standards:
	+ Secure and maintain wireless connections in compliance with current technical and physical security standards.
	+ Do not connect WAPs directly to [EMPLOYER'S NAME]'s trusted network without protective controls, such as a firewall.
	+ Deactivate WAPs when not in use, including during non-business hours.
* Handling highly confidential information:
	+ Use appropriate protective measures, including encryption, when transmitting or receiving highly confidential information over Wi-Fi.
	+ Contact the Information Security Coordinator for guidance on secure Wi-Fi practices when handling highly confidential information.
* Device standards:
	+ End-user devices accessing wireless networks (e.g., laptops) must have personal firewalls installed and maintained according to current standards.
	+ Deactivate the wireless networking interface on devices when not in use.

**PROTECTING AND MANAGING [EMPLOYER’S NAME]’s INFORMATION TECHNOLOGY ENVIRONMENT**

Protecting information assets

[EMPLOYER'S NAME] configures and maintains its IT hardware and software according to current technical standards, including the installation of anti-malware tools, operating system updates, and security patches. Preventive controls help prevent unauthorized activities or data access, while detective controls monitor and respond to unauthorized actions in real time.

End-user computers and access

* All end-user devices must authenticate with [EMPLOYER'S NAME]'s domain at startup and user login. Devices not meeting software or configuration standards may be denied network access.
* User accounts must utilize strong passwords and multifactor authentication (MFA). Accounts may be deactivated after [NUMBER] failed login attempts, with reactivation based on technical feasibility and risk.
* Remote access points must use MFA, and all authentication credentials must be encrypted during transmission.

Password and user credentials

Passwords and other user credentials are critical to securing systems and must be protected rigorously. Passwords must meet these minimum criteria:

1. At least [LENGTH] characters.
2. A mix of uppercase, lowercase, numbers, and special characters.
3. Avoidance of dictionary words, predictable patterns (e.g., "qwerty"), or personal information.

Techniques such as mnemonic phrases can help create strong, memorable passwords. Treat passwords as highly confidential information and change them periodically or immediately if compromised.

Protect passwords and authentication credentials by:

* Never sharing them with others or recording them insecurely.
* Avoiding saved password features unless approved by [EMPLOYER'S NAME].
* Using unique passwords for each system or account unless automated single sign-on is enabled.

Perimeter controls

[EMPLOYER'S NAME] employs firewalls and other perimeter controls to separate its trusted network from external environments. Additional measures, such as intrusion detection, data loss prevention, and network monitoring, may be used based on risks.

Data and network segmentation

Highly confidential information must be segmented from other parts of [EMPLOYER'S NAME]'s network using firewalls, access control lists, and similar mechanisms. Do not modify segmentation plans without approval from the Information Security Coordinator.

Encryption

Encryption protects both data-at-rest and data-in-transit. Only use approved encryption algorithms and tools. Periodically review encryption methods to ensure security, and adhere to export laws when dealing with encryption technologies.

Treat encryption keys as highly confidential information. Use secure storage, maintain backups, and ensure keys are accessible when required. Rotate encryption keys periodically to mitigate risks.

Data and media disposal

When retiring IT equipment or storage media containing confidential or highly confidential information, ensure data is rendered unreadable through physical destruction or data-wiping tools that comply with standards such as NIST SP 800-88.

Log management and retention

System and user activity logs must be secured against tampering and reviewed regularly to identify potential security incidents. Retain logs in accordance with [EMPLOYER'S NAME]'s [Records Retention Schedule/[RECORDS POLICY NAME]].

**PHYSICAL (ENVIRONMENTAL) SECURITY**

[EMPLOYER'S NAME] employs physical safeguards to protect information assets from theft, intrusions, unauthorized use, or abuse. All employees and authorized users must follow the organization's physical security policies and procedures (refer to [[EMPLOYER'S NAME] Physical Security Policy/[PHYSICAL SECURITY POLICY NAME]]) and adhere to the following guidelines:

1. Screen placement: Position computer screens so that unauthorized parties cannot view the displayed information.
2. Visibility of confidential data: Do not display confidential or highly confidential information on screens visible to unauthorized individuals.
3. Workstation security: Log off or shut down your workstation when leaving for an extended period or at the end of the workday.
4. Secure server locations: Store servers and other computing or network equipment (excluding end-user devices) in secure data centers or other areas approved by the Information Security Coordinator.
5. Network cabling: Avoid running network cabling through unsecured areas unless it only carries Public Information or is otherwise protected, such as with encryption.
6. Deactivation of unused network ports: Deactivate any network ports not in use to prevent unauthorized access.
7. Storage of end-user devices: Store end-user devices not in use for extended periods in secure areas or securely dispose of them in compliance with this policy.

**DISASTER PREPAREDNESS**

[EMPLOYER'S NAME] establishes, maintains, and tests disaster preparedness plans to ensure continuity of operations and system availability in the event of a disaster or other unplanned, business-impacting event. These plans are developed, reviewed, and tested in accordance with [[EMPLOYER'S NAME]'s Business Continuity Planning Policy and Procedures/[DISASTER PREPAREDNESS POLICY NAME]]. All disaster preparedness plans are classified as confidential information.

Backup and restoration

System administrators must conduct regular data backups for the information assets they manage, following [[EMPLOYER'S NAME]'s Backup Policy and Procedures/[BACKUP POLICY NAME]]. When designing a backup strategy, consider:

1. The business criticality of the data.
2. The resources required for backups.
3. The impact on users and network resources.

Backups must be safeguarded according to the classification level of the stored data. Restoration procedures should be documented and periodically tested to confirm reliability and readiness in the event of a disaster.

**MANAGING INFORMATION ASSETS**

[IT/[IT ORGANIZATION NAME]] oversees IT operations and related activities within [EMPLOYER'S NAME]. Only approved or [EMPLOYER'S NAME]-supplied hardware, software, and systems may be installed or connected to the organization's IT environment. Changes to the production IT environment must be approved and managed by [IT/[IT ORGANIZATION NAME]] to avoid unexpected disruptions. For any questions about IT operations, contact [IT CONTACT]. Development environments must align with this Policy and current [IT/[IT ORGANIZATION NAME]] standards to mitigate security risks.

Procurement

Only [IT/[IT ORGANIZATION NAME]] or authorized personnel may procure information assets for use within or connection to [EMPLOYER'S NAME]'s network. This applies to all software or hardware, whether purchased, open-source, or provided free of charge.

Involve the Information Security Coordinator early in the development process to manage security risks.

Authorization from Legal and the Information Security Coordinator is required before using cloud services to manage confidential or highly confidential information.

Asset management

All information assets, including hardware, software, and related equipment, must be tracked and documented using [EMPLOYER'S NAME]'s asset management system(s).

* Include details like operating system levels and installed software versions to aid vulnerability management.
* Update inventory records when assets are retired or removed.
* Assign a data owner to confidential or highly confidential information, responsible for tracking its location, use, and disclosure.
* Dispose of data and media securely to prevent breaches.

Authorized environments and authorities

Only authorized personnel from [IT/[IT ORGANIZATION NAME]] or approved project teams may install or connect hardware or software within [EMPLOYER'S NAME]'s IT environment.

* Do not convert end-user devices into servers or shared resources without [IT/[IT ORGANIZATION NAME]] assistance.
* Limit administrative or privileged access to individuals with a clear business need.
* Administrative access and processes must be distributed across multiple individuals to reduce risk.
* New or modified internet connections and internet-facing environments must be approved by the Information Security Coordinator.

Change management

[IT/[IT ORGANIZATION NAME]] maintains a change management process to reduce business disruptions when altering [EMPLOYER'S NAME]'s production IT environment.

* Change requests must include:
	+ Assigned roles and responsibilities.
	+ Implementation milestones.
	+ Testing procedures.
	+ Rollback plans in case of failure.
* During software development, track problems, fixes, and releases using a change management process. Use versioning tools to archive code for recovery if needed.

Application and software development

To avoid unintended impacts on production environments, application and software development, including system testing, must occur in segmented environments.

* Segregate duties between development and operations. Developers may have limited access to production environments only for specific troubleshooting or support needs.
* Follow security-by-design principles to address risks early in development.
* Consult the Information Security Coordinator, vendors, and industry best practices to mitigate application-level security risks.
* Prioritize protecting highly confidential information through encryption or equivalent safeguards.
* Implement defensive coding techniques, regular code reviews, and application-level scanning to identify and address vulnerabilities before software release.

**INCIDENT REPORTING AND RESPONSE**

The Information Security Coordinator oversees the cyber incident reporting and response process, ensuring proper notifications are made based on the incident’s severity. All reported or detected incidents are investigated, and outcomes, including mitigation and remediation steps, are documented.

Incident reporting

If you discover or suspect a breach of [EMPLOYER'S NAME]'s information security controls, immediately notify [CONTACT]. While monitoring systems are in place, you may be the first to notice an issue. Prompt reporting helps mitigate damages and reduces further risk to the organization.

Treat all information related to cyber incidents as highly confidential and do not share it internally or externally without explicit authorization.

Examples of cyber incidents

Report any of the following cyber incidents:

1. Loss or suspected compromise of user credentials or physical access devices, such as passwords, tokens, badges, or smart cards.
2. Suspected malware infections (e.g., viruses, spyware, Trojans, worms), or unusual alerts from anti-malware software or firewalls.
3. Loss or theft of devices containing [EMPLOYER'S NAME]'s information (e.g., laptops, smartphones, USB drives).
4. Suspected unauthorized access (hacking) to [EMPLOYER'S NAME]'s systems or network.
5. Breach or suspected breach of confidential or highly confidential information.
6. Attempts to obtain sensitive information through social engineering (e.g., phishing emails or fraudulent phone calls).
7. Any situation that violates this policy or creates risks to [EMPLOYER'S NAME]'s information assets.

Compromised devices

If you suspect a device is compromised:

1. Immediately disconnect the device from the network but do not power it down to preserve forensic data.
2. Notify [CONTACT] right away.

Incident management

The Information Security Coordinator maintains a cyber incident response plan to address reported incidents. Once an incident is reported, follow the incident response process and do not take independent action or conduct your own investigation unless specifically authorized by the Information Security Coordinator.

Data breach notification

Applicable laws may require [EMPLOYER'S NAME] to notify authorities, affected individuals, or organizations if certain types of information are exposed or lost (e.g., highly confidential or personal information). Notifications may also be required for incidents affecting critical services or infrastructure.

The Information Security Coordinator’s incident response plan includes a review step to determine whether notifications are required. All external notifications must be coordinated with Legal and the Information Security Coordinator. Do not make any external notifications without prior authorization.

**SERVICE PROVIDER RISKS AND GOVERNANCE**

The Information Security Coordinator oversees a service provider risk governance program to manage risks associated with service providers that interact with [EMPLOYER'S NAME]'s systems or access confidential or highly confidential information. This program includes processes for tracking service providers, assessing their capabilities, and periodically evaluating their compliance with this policy.

Service provider approval required

Before engaging a service provider for tasks involving access to [EMPLOYER'S NAME]'s systems or confidential or highly confidential information, you must obtain approval from Legal and the Information Security Coordinator.

Contract requirements

Service providers with access to [EMPLOYER'S NAME]'s systems or sensitive information must agree to comply with applicable laws and this policy (or equivalent security measures) as part of their contract.

[EMPLOYER'S NAME] may also require service providers to demonstrate compliance through independent audits, certifications, or other reviews based on risk assessments.

**CUSTOMER OR CLIENT INFORMATION**

[EMPLOYER'S NAME] frequently creates, receives, and manages data on behalf of its [customers/clients]. Each business unit, with guidance from the Information Security Coordinator, must develop, implement, and maintain processes to handle [customer/client] data intake and protection. These processes must:

1. Identify [customer/client] data and any relevant requirements prior to data intake or creation.
2. Maintain an inventory of created or received [customer/client] data.
3. Ensure the implementation of appropriate security measures, including secure disposal of data and media when no longer needed for business purposes or as required by [customer/client] agreements.

Requirements identification

Before creating or receiving [customer/client] data, identify all relevant requirements based on your business unit's data intake process. These requirements may be contractual, legal, regulatory, or a combination of these.

Intake management

Each business unit's [customer/client] data intake process must ensure secure data transfer and maintenance of an inventory that includes:

* A description of the data and its intended use.
* The location(s) where the data is stored.
* Authorized access roles or categories.
* Data classification as confidential or highly confidential Information.
* Retention duration or criteria.
* Specific contractual, regulatory, or other obligations related to data protection and management.

Treat all personal information provided by [customers/clients] as highly confidential information. Engage in ongoing discussions with [customers/clients] to assess whether business objectives can be achieved without transferring personal information to [EMPLOYER'S NAME].

Customer/client data protection

Protect all [customer/client] data created or received in compliance with this policy, the data's classification level (confidential or highly confidential), and any client-specified requirements.

Customer/client data and media proposal

Securely dispose of any [customer/client] data or media containing such data when it is no longer needed for business purposes or as dictated by [customer/client] agreements. Update the business unit's [customer/client] data inventory to reflect the disposal.

**ACKNOWLEDGEMENT OF RECEIPT AND REVIEW**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (employee name), acknowledge that on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date), I received and reviewed a copy of [EMPOYER'S NAME]’s [NAME OF POLICY]. I understand that it is my responsibility to familiarize myself with the policy and adhere to its terms.

I also acknowledge that this policy is not intended to create an employment contract or alter my at-will employment status, unless otherwise specified in a written agreement signed by an authorized representative of [EMPOYER'S NAME]. Any delay or failure by [EMPOYER'S NAME] to enforce the provisions of this policy does not constitute a waiver of its rights to enforce them in the future.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date