Security Policy

Instructions

This template is a starting point to enable you to create a Security Policy tailored to meet the needs of your organization. Perform a full document replacement of **<Organization>** with the proper name of your organization.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Contents

Purpose of the Policy

This Information Security Policy ("Policy") expresses **<Organization>**'s commitment to managing information security risks effectively and efficiently, coordinated globally and in compliance with applicable regulations wherever it conducts business.

This Policy is the foundation for all information security activities. It focuses not only on the technology for the storage, processing, and transmission of information, but also on administrative and operational practices for the protection of all information, data, files, and processing resources owned by **<Organization>**.

It is the intent of this Policy to facilitate the exchange of information and computing resources while balancing the need for protecting information with the cost of implementation.

This Policy is the property of **<Organization>**. It is intended for distribution to all employees and users of information systems at **<Organization>** locations.

Scope of the Policy

This Policy applies to all employees, vendors, contractors, and consultants, who create, distribute, access, or manage information by means of **<Organization>**'s information technology systems including personal or corporate computers, networks, and communication services by which they are connected. It equally applies to individuals and enterprises, who by nature of their relationship to **<Organization>**, are entrusted with confidential or sensitive information.

This Policy addresses all aspects of information security and continuity from initial design of a system through implementation and operation. It also addresses any device used to store, process, or communicate **<Organization>** proprietary or other protected information.

Definitions

Information Owner – Information Owners are the managers who bear responsibility for the acquisition, development, and maintenance of applications that process **<Organization>** information. All application and company information must have a designated Information Owner. For each type of information, Information Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilized.

Custodians – Custodians are in physical or logical possession of either **<Organization>** information or information that has been entrusted to **<Organization>**. While System Administrators are Custodians, whenever information is maintained only on a personal computer, the User is also a Custodian. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by Information Owners.

Information Users – Information Users ("Users") include all employees of **<Organization>** who access or receive information produced, stored, or communicated by **<Organization>**'s information technology systems. Users also include all individuals, who by nature of their relationship with **<Organization>** (e.g. contractors, vendors, service providers, consultants, etc.) are entrusted with sensitive or confidential information. Users are responsible for compliance with the Information Security Policy and individual Standards and Procedures.

Policy Requirements

If any of the following requirements in this policy cannot be met, then that security exemption must be documented and recorded. Exemptions must be reported to the Security Officer.

Security Management

The security of corporate information, applications, systems, and networks is fundamental to the continued success of **<Organization>**. Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information. Security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of **<Organization>** information, applications, systems, and networks for authorized Users.

Confidentiality

Confidentiality relates to the protection of information from unauthorized access regardless of where it resides or how it is stored. Information that is sensitive or proprietary needs to be protected to a higher level than other information. See *Information Classification and Handling Policy* for further guidance.

Integrity

Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Users accessing sensitive information, applications, systems and networks must be identified and authenticated.

Availability

Availability is the assurance that **<Organization>** information and resources are accessible by authorized Users as needed. There are two issues relative to availability: denial of services caused by a lack of security controls (e.g. destruction of data or equipment, computer virus), and loss of services from information resources due to natural disasters (e.g. storms, floods, fires). See *Business Continuity Planning Process* for more information about how this can be addressed.

Authentication

Authentication requires that the origin of a message be correctly identified with assurance that it is not a false or forged identity. Passwords are used to authenticate a User based upon the fact that only the User should know the password. Strong passwords will be used and must contain a number of rules such as combinations of letters and numbers with combinations of upper and lower cases. One-time passwords will also be implemented for high-risk applications as well as encryption to provide the authentication security service to identify the origin of messages. In addition to the use of passwords, Multi-factor Authentication must be implemented where is it possible and appropriate.

Information Assets

All information, data, applications, networks, and equipment are the property of **<Organization>** and are provided to its employees so that they can conduct their job responsibilities effectively. These assets should be treated with privacy and confidentiality in line with the Information Classification and Handling Policy when conducting business and should not be made available or accessible to anyone outside the enterprise without specific written permission of the Chief Information Officer.

<Organization> information and information processing infrastructure are vital assets requiring protection commensurate with their value. Organizational information, applications, systems, and networks must be actively managed to ensure security, confidentiality, integrity, and availability.

Accountability

<Organization> administrative and computing environments will maintain consistent standards for establishing the accountability and authenticity of system Users, which will be compatible with internal accounting control standards prescribed by **<Organization>**.

These environments will develop unique standards for protecting information, applications, systems, and network resources contained within these environments that will be commensurate with fulfilling the mission of **<Organization>** and maintaining the integrity of those critical resources.

To maintain accountability for system access, **<Organization>** will implement the following:

- All individuals with access to the systems will use a User ID that has been authorized by company management and specifically assigned to that individual. Sharing of User IDs is prohibited except in specific, approved situations.
- All individuals with network, system, and application User IDs will retain a confidential password that will be used to authenticate the identity of the individual. Intentional disclosure or sharing of passwords is prohibited.

Information Access

All access to information is to be authorized by information owner, with access granted or revoked based on business requirements only. Access to administrative data will be granted to **<Organization>** employees only. Individuals outside of **<Organization>** can be authorized access to **<Organization>** data only if that authorization is granted by the Information Owner.

Access and update capabilities/restrictions will apply to all **<Organization>** data, stored company computing facilities. Security measures apply to all systems developed and/or maintained by **<Organization>** organizations, affiliates, outside vendors, or contractors.

The appropriate Head of Business Unit and the System Administrator are responsible for authorizing access to systems and information, verifying information integrity, and controlling extracted information. Management is responsible for developing secure processing systems and operating these systems in a controlled environment. Employees are required to comply with management's direction for the use and protection of information technology processing systems and information.

Employees must be kept aware of the importance of information security. All managers and employees are required to act with urgency and diligence to fulfill these requirements.

Risk assessments must be carries out and identified risks must be evaluated to determine the optimum level of control required for each type of information technology system. Adequate controls are to be included to ensure that information security, confidentiality, integrity, and availability are achieved.

Policy Responsibilities

Security Officer

The Security Officer of **<Organization>** has overall responsibility for information security matters. These responsibilities are to:

- Ensure appropriate User access and authentication controls are in place.
- Ensure that the documented security policies, standards, and procedures are reviewed, updated, and maintained periodically by appropriate individuals.

- Evaluate security exposures, misuse, or non-compliance situations and ensure implementation of security controls to address those incidences.
- Ensure that employees execute their security responsibilities in accordance with related policies, standards, and procedures.
- Develop and implement the Security Awareness Program.

Information Resources

Information resources including computer software and support systems should be protected appropriately to maintain the sensitivity and critical nature of information that is processed, stored, or communicated. Information systems should be protected in such a manner to ensure that unauthorized persons are not able to directly access the device and either cause physical damage or modify internal components that could affect the results of computing or other processes.

Environmental and security controls should be appropriate for the level of risk. An assessment that balances risk with the cost of implementing the control should be completed when determining what security and environmental controls are appropriate.

Users are responsible for adhering to copyright, patent laws, and license agreements for intellectual property.

Communication facilities and equipment should be protected from unauthorized modification and tampering to ensure that messages in transit are not modified or received by unintended parties or that communication services are not interrupted. Communication facilities can include all equipment rooms and wiring closets and may include facilities and resources provided by third-party service providers.

Questions concerning the appropriateness of physical and environmental controls should be addressed to the Security Officer.

System and Information Ownership

<Organization> is the owner of all information, applications, systems, and software that are developed, used, or distributed to employees or designated representatives of entities operating as business partners. Although **<Organization>** maintains the ultimate ownership responsibility, certain managers are responsible for executing this responsibility.

Systems and information owners are responsible for identifying and managing risks relating to the security, integrity, and continuity of information, and for the business processes and system functions that create, modify, delete, or use this information. They are responsible for assessing the level of risk to **<Organization>** for providing access to information, as well as for determining the impact to the organization if information, business processes, or system functions were not available or if they are misused.

The level of security, integrity, and continuity risk needs to be communicated by the owner to individuals or groups responsible for implementing **<Organization>** security and business continuity controls.

Periodically, the Information Owner and the Security Officer will review the current set of accesses and update capabilities granted to each individual on the system in order to ensure that the appropriate level of access has been granted and that no changes are necessary.

Risk assessments must be presented to the Security Officer.

Access to Systems and Information

<Organization> commits to the principle of least privilege and as such will conduct access reviews to ensure Information Custodians do not have excessive access.

All access to systems and information is provided based on business need. Information owners, as part of their management responsibility, are required to authorize requests for access to information or systems, and to verify that such access meets a legitimate business need, prior to access being implemented.

An Access Request Form will be completed and will indicate the system or information access that the User should be permitted. This form will be authorized by a Head of Business Unit or the Information Owner as required.

Access to sensitive information needs to be restricted. Owners may also designate a retention period during which the information or access may be authorized and after which all access is to be revoked.

When approval for outside access to **<Organization>** information is granted, instructions must be provided to the recipient notifying them of any security requirements, including the need to maintain the confidentiality of the information, requirements for distribution of the information within their organization, and procedures for destruction or return of the information following the period of access. All non-employees will sign a Non-disclosure Agreement.

All employee, contractor, vendor, and consultant User IDs must be disabled without delay upon their leaving the company.

When a Head of Business Unit is notified of an employee termination/resignation, they should review the disposition of the User's data and files with the User prior to separation from **<Organization>**.

Security Monitoring and Enforcement

It is the responsibility of the Security Officer to implement appropriate measures to detect attempts to compromise the security or integrity of information or information technology systems. When implementing monitoring capabilities, consideration should be given as to what situations are to be monitored based on the extent of risk, the most effective means for monitoring security activities, the resources available for monitoring, and system constraints that limit the ability to monitor security events. If appropriate measures are not available within a system environment to effectively monitor security events, additional controls to mitigate security risks should be implemented.

When activity occurs that is in conflict with security policies and standards, Head of Business Units should take the appropriate steps to enforce desired security practices. The steps involved range from training of the Users, revoking access, altering security parameters and possibly disciplinary actions.

Due to the likelihood of damage and destruction of information resulting from malicious code, including viruses, detection capabilities must include malware detection software within the local area network environment, as well as on systems that are at high risk for infection.

Security Awareness Program

It is the responsibility of management to ensure that all Users of information understand how to protect company assets, including information and information resources and comply with security policies, standards, and procedures. Supervisors and managers must ensure that persons working within their department understand general information security requirements and they are sufficiently knowledgeable about the information technology security policies, standards, and procedures to recognize the need for protecting information and the requirements for which they are specifically responsible.

The Security Officer is responsible for developing and implementing an Information Security Awareness Program that supports employee awareness. Managers need to be aware of User performance in this area, encourage good security practices, and address inappropriate behavior.

Computer Security Incident Response

<Organization> shall develop effective plans and procedures for responding to suspected information security incidents that affect the confidentiality, integrity, or availability of data processed or owned by **<Organization>** or for which **<Organization>** serves as a custodian.

These plans and procedures shall address the following stages of incident response:

a. Preparation
b. Detection and Reporting
c. Analysis
d. Containment
e. Recovery
f. Post-Incident Activities

The facts surrounding an intrusion, infection, or system compromise must be documented, reported to the Security Officer, and include the circumstances that led to the discovery of the incident, actions which were immediately taken, the names of persons involved in investigating the incident, and detailed observations about what transpired, what damage was caused, and what systems or files were compromised.

Disaster Recovery/Business Continuity Planning

Should the confidentiality, integrity or availability of systems or information be affected by an incident, it is the responsibility of management to ensure that planning and preparation is performed to minimize loss, reduce impact, and ensure continuity of the organization's functions and revenue stream. A Business Continuity Plan (BCP) will be developed and tested for effectiveness. The BCP will address pre-planning risk control, crisis management, and business recovery.

Compliance

<Organization> complies with all applicable federal, state, provincial, local, industry and contractual regulations.

Non-compliance or violation of this policy should be brought to the immediate attention of the Security Officer. The Security Officer will work with company management and System Administrators to ensure that the problem is resolved and to address necessary steps to eliminate future violations. An escalation process will define the course of action for all violations consistent with the severity of the violation.

<Organization> reserves the right to discipline, terminate, suspend, or prosecute, at its discretion, individuals who violate the information Security Policy.

Service Delivery

<Organization> promotes secure practices in delivery of its products and services through awareness, training and industry best practices.

Physical and Environmental Security

<Organization> maintains controls to limit access to physical assets and mitigates risks associated with environmental issues (fires, floods, power loss) to help ensure data protection and system availability.

Delivery Partner Management

<Organization> ensures processes exist to evaluate the service capability of potential business partners through:

- Non-disclosure agreements.
- Due diligence, including references, accreditations, etc.

<Organization> monitors partners and suppliers to ensure defined service objectives are met.

<Organization> ensures processes exist for vendor termination that provide minimal disruptions and maintain data confidentiality.

Additional Policies

[Instructions] You can attach additional issue-specific policies to this Security Policy and list them below. A list of possible issue-specific policies is shown.

The following policies pertain to specific topics or issues and are attached. These issue-specific policies shall be considered part of this Security Policy and are subject to the same provisions:

a. Acceptable (Computer) Use Policy
b. Desktop Configuration Policy
c. Remote Access Policy
d. Information Lifecycle and Disposal Policy
e. Laptop and Mobile Device Policy
f. Backup and Disaster Recovery Policy
g. Business Continuity Policy
h. Physical Security Policy
i. Wireless Network Security Policy
j. Password Policy
k. Personnel Security policy
l. Update / patching policy
m. Web application policy
n. Incident Response Policy
o. Privacy Policy
p. Information Lifecycle and Disposal Policy

Policy Review

This policy and supporting Information Security policies will be reviewed annually and updated as required.

Acceptable Use Policy

Instructions

This template will enable you to create an Acceptable Use Policy that meets the needs of your organization.

Acceptable Use Policies (AUPs) are unique. They are generally the only policies that directly affect every person in the organization. They are also the only policies that every employee and every contractor who has access to computing systems should be required to sign.

In the policy requirements section there are a number of statements, not all of which will apply to your organization. These can be freely modified or deleted. The organization must decide what is or is not acceptable use of its computing resources. Sections that refer to illegal acts, or acts for which the organization could be held liable, will likely need to be included in the AUP.

Perform a full document replacement of **<Organization>** with the proper name of your organization. Areas within the template that are required to be reviewed and changed are highlighted.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Contents

Purpose of the Policy

The purpose of this policy is to outline the acceptable use of information systems and computing equipment at **<Organization>**. These rules are in place to protect the employee and **<Organization>**. Inappropriate use exposes **<Organization>** to risks including malware attacks, compromise of network systems and services, loss of confidential information, and legal issues.

Scope of the Policy

This policy applies to all **<Organization>** devices, employees, and contractors. All employees and contractors with access to **<Organization>** computing devices or information systems shall comply with this policy as it applies to their job duties. This policy also applies to documents and systems including but not limited to:

1. Hard Copy Documents (e.g Printed Reports, White Mail, Faxes).
2. Computer Systems (e.g Desktops, Servers, Storage Networks).
3. Mobile Electronic Devices (e.g Laptops, tablets, smart phones).
4. Removable Storage Devices.
5. Telephone Systems (e.g PBX, VOIP, voice recording and transcription services).
6. Printer, Fax and Photocopier Systems.
7. **<Organization>** Offices and Data Centres.

Definitions

Protected Information is information that is highly sensitive and that must be safeguarded in accordance with legislative or regulatory requirements. Protected Information is often subject to privacy breach notification laws, and the loss of this information could have severe consequences for the organization. Examples include Protected Health Information, Payment Card Information and most forms of Personally Identifiable Information (PII).

PII (Personally Identifiable Information) is defined in NIST Special Publication 800-122 as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Confidential Information is information owned by the organization or entrusted to the organization that is not intended for sharing with the public. Security protections must be applied to this information to safeguard its confidentiality, integrity and availability.

Responsibility for Policy Implementation

The**<Organization>** Security Officer or other authorized representative shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

General and Internet Use

Employees and contractors shall not, under any circumstances, use **<Organization>** computing devices or information systems to:

1. Engage in any activity that is illegal or violates the rights of any person.
2. Download or install software of any type on **<Organization>** computing devices without authorization.
3. Copy or distribute any copyrighted material without authorization.
4. Access the personal information of others without authorization, except as part of the employee's or associate's assigned duties.
5. Make any claims on behalf of **<Organization>** unless authorized to do so.
6. Associate **<Organization>**'s name with any activity that would harm the reputation of the organization.
7. Visit websites exhibiting sexually explicit material, gambling sites or sites related to illegal activities.
8. Visit websites that encourage discrimination or the violation of the rights of any group or individual, except in the course of authorized research.
9. Visit websites which share music or other files on a peer-to-peer basis, or otherwise share content in violation of copyright laws.
10. Engage in any activity that interferes with the ability of another organization or individual to conduct computing activities (e.g. denial of service attacks).
11. Provide information about **<Organization>** or its employees, clients, customers, patients, or associates to any outside party, unless explicitly authorized to do so.
12. Post comments or other information to social networking sites or blogs on behalf of, or using the name of the organization, unless explicitly authorized to do so.

Personal Internet Use

Activities of a personal nature such as non-business online shopping, access to personal email, job searching and access to personal pages of social networking sites are [prohibited] or [permitted only during the hours listed below] or [permitted, within the limitations of this policy] or [permitted, subject to the restrictions listed below]. Work related to accessing official **<Organization>** information is not personal use of the internet and is an exception. [Add additional restrictions for Internet use or hours designated for personal Internet use here.]

Online File Sharing, Backup and Synchronization Services

Online file sharing, backup and synchronization services, such as Dropbox, Google Drive, OneDrive, etc. are very convenient ways to store and share files online but increase the risk that Confidential Information or Protected Information will be inappropriately shared. The following controls must be followed:

1. Protected Information [and Confidential Information] must not be copied to or stored on any online file sharing or backup system without specific authorization from the Security officer or other authorized **<Organization>** representative.
2. Use of online file sharing, backup and synchronization services for information that is not Protected Information is [prohibited] or [restricted to the following services]: [List approved file-sharing services here. You should restrict file sharing to specific services or to one service. Allowing the use of multiple services increases the risk of information leakage.]

Transmission of Protected Information
Employees and contractors must not transmit any Protected Information in any email or via any instant messaging or chat service.

All Protected Information must be transmitted via a secure file transfer method.

Authorized Storage Locations for Protected Information
All Protected Information shall be processed and stored within the applications authorized by the organization. No employee or contractor may copy any Protected Information to any other location unless directed to do so by an authorized **<Organization>** representative.

Email Usage
Email is an important communication tool, but also has the potential to cause damage to the organization. Inappropriate use of email can result in the loss of sensitive or company confidential data or intellectual property, damage to public image, damage to critical internal systems, and unintentional employee exposure to inappropriate content or material.

<Organization> employees and contractors must not engage in any of the following:

1. Sending unsolicited email messages, including sending “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Harassment in any form, whether through language, frequency, or size of messages.
3. Creating or forwarding “chain letters” or “Ponzi” or other “pyramid” schemes of any type.
4. Sending similar email messages from multiple email addresses with the intent to harass or elicit replies.
5. Using unsolicited email originating from within the organization’s networks or other Internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by the organization.
6. Posting the same or similar non-business-related messages to large numbers of internet posting sites.
7. Unauthorized use, or forging, of email header information.

Instant Messaging
The **<Organization>** does accept that employees may use their **<Organization>** email and Instant Messages (IM), such as WhatsApp, for a reasonable degree of acceptable personal use, providing such use does not contravene any part of this policy. If usage is deemed to be excessive, the individual will be notified and may be subject to disciplinary action.

Email and IM sent from **<Organization>** accounts are legally classed as formal business records and could therefore be disclosed to third parties during litigation or criminal investigation. Employees must therefore always exercise caution when sending messages to third parties. Be careful not to include language that could represent an agreement, contract or offer. Employees need to be aware that deleted messages may also be retrievable and admissible during litigation and incident investigation.

IM must not be used to conduct business, other than to arrange meetings and calls.

Employees must exercise caution when expressing personal opinions or views via email and IM. Language used should always remain polite and respectful.

Scams and hoaxes are communicated via email and IM and often include viruses and other malware aimed at stealing sensitive information. Therefore, employees must exercise extreme caution when opening attachments. Any suspicious messages should be deleted and reported immediately.

Downloading or Installing Software

<Organization> employees and contractors may not download or install any software application without the authorization of an authorized company representative.

Social Media

Social media sites are places on the internet where people can share information, interact and communicate with each other (e.g. Facebook, LinkedIn, and Twitter). Social media can be a valuable tool for the promotion of the organization, its goals, and its values. It can also be used as a means of sharing valuable information for the purpose of helping others

improve security and reduce risk. However, messages posted to social media sites must be carefully considered, because once posted, these messages cannot be recalled or removed easily, if at all.

No employee or contractor shall post to any social media site on behalf of the organization or purport to represent the organization in any way, without authorization.

<Organization> respects the right of individuals to use personal websites and social media sites as a medium of self-expression. However, the posting of any material that may damage or undermine the reputation of the **<Organization>** and its employees may be subject to disciplinary action. All employees and contractors who are authorized to post to social media sites on behalf of the organization must adhere to the following standards:

1. Be respectful of the organization, as well as its employees, associates, and competitors. Do not post derogatory, malicious, demeaning, insulting or inflammatory comments about anyone or any organization.
2. Use the first person (I, not we) and always appropriately identify yourself.
3. Be accurate.
4. Cite source material. If you have obtained information from an online or other resource, cite the source. If possible, cite the original source. If you are stating an opinion, rather than a fact, make sure this is clearly represented.
5. Clearly state that your opinions are your own, and that they are not the official opinions of **<Organization>**.
6. Do not use profanity, ethnic slurs or abusive language.
7. If you make an error regarding facts, post a correction or retraction as soon as possible.
8. Protect confidential or proprietary information and information that relates to a personal matter within the workplace. Do not identify coworkers, clients, business partners or suppliers without permission.
9. Do not use copyrights, trademarks, or logos without permission.
10. Be professional. Any blog or social media posting that mentions or can be associated with **<Organization>** becomes a part of the organization's public image. Restrict your comments to those subjects about which you have knowledge.
11. Make sure your posts are making a positive contribution to both the organization's image and to your personal image as an employee or contractor.
12. Do not create links to any **<Organization>** website without authorization from the **<Organization>**.
13. Do not copy **<Organization>** trademarks, logos or material without permission from the **<Organization>**.

<Organization> employees must not engage with any media regarding unauthorized release of any **<Organization>** or client information or data. Any requests for information, data or views on the **<Organization>** or clients are to be directed to XXX for guidance.

Remote Access and Personal Wireless Networks

No employee or contractor is permitted to install any wireless networking device that connects to the organization's systems without authorization from the IT administrator, or other appropriate party.

No employee or contractor may install any software or application that allows access to the organization's systems from a remote location without appropriate authorization from **<Organization>**.

Reporting Security Incidents

All employees and contractors must report the following as security incidents to the Security Officer or another authorized **<Organization>** representative:

1. Any observed unauthorized disclosure of Protected Information or Confidential Information, whether intentional or unintentional.
2. Any observed attempt to view or access Protected Information or Confidential Information beyond by a person not authorized to view or access that information.
3. Any unauthorized attempt to gain physical access to, or install unauthorized software applications on, any server or workstation.
4. Any telephone, email, or other communication that include an unauthorized attempt to receive or access Protected Information or Confidential Information.
5. Any unusual computer behavior (unusual error messages, unusual pop-up windows, website redirection, etc.). When unusual computer activity is observed, the computer should not be turned off to preserve valuable evidence. The Security Officer or other authorized **<Organization>** representative should be contacted immediately.

Protecting the Organization from Cyber Threats

Phishing and "social engineering" attacks: Sooner or later you will be the target of an attempt to trick you into disclosing Protected Information or Confidential Information or installing malicious software on **<Organization>** systems. Be aware that social engineers often conduct extensive research in preparation for their attacks and may present you with names, events, or other information that you would not expect to be known to anyone outside your organization. Be aware of the following considerations:

1. Exercise caution with email attachments and links in email messages. If the message is unexpected or if you have any doubt about whether it is genuine, contact the sender. Do not reply to the email. Contact the sender using contact information you have previously recorded.
2. Be suspicious if anyone asks you for a password, account information, or other confidential information. Phishing email messages can be made to look exactly like legitimate messages you have received in the past.
3. Never send Protected Information or Confidential Information, enter passwords, or provide account information over an insecure connection. A secure connection will always start with https:// in the browser address bar.
4. Do not click on banner ads or the ads along the top, sides, or bottoms of web pages. These ads are designed to be tempting, but some may link to malicious websites.
5. Understand that you will be targeted by cyber-criminals and that they want to steal confidential information from all businesses, both large and small. Be constantly vigilant.

User credentials such as usernames, passwords and PINS that are used to identify and authenticate the users of a system must be protected. Poor management of such credentials will put sensitive information at risk and the owner of the credentials could be held personally liable for any actions carried out by an individual using their credentials. To protect user credentials, employees:

1. Must keep passwords and PINs secret – They must not be written down or given to anyone else.
2. Should change their passwords at least every 90 days.
3. Must change passwords and PINs on suspicion that someone else may know them.
4. Must use a combination of letters, numbers and symbols when selecting a new password.
5. Should select passwords of at least 12 characters in length where systems allow it, with a mixture of upper and lower-case characters and symbols.
6. Must not re-use a previous password.

Implementing effective physical security controls is essential in protecting sensitive information. When on **<Organization>** premises, employees:

1. Must use their building pass to access the premises;
2. Must ensure only authorized employees enter the premises, challenge anyone who is not recognized, or that you believe does not have a legitimate reason to be onsite;
3. Must report any suspicious person, or activity to the building's security or management;
4. Must not share, or lend their building access pass to any other person; and
5. Must not access the building without a building pass by tailgating others, instead they must report to Reception.

The **<Organization>** enforces a "Clear Desk Policy" as an effective way of minimizing the risk of unauthorized information loss. To meet this policy, employees:

1. Must clear their desk areas of sensitive information and lock it away at night;
2. Must lock their computer when leaving it unattended;
3. Must collect sensitive printer and photocopier output promptly;
4. Must clear notice boards and flip charts of sensitive information after meetings; and
5. Must not leave unattended valuable information and items on clear display.

Acknowledgment

I have read, understand, and agree to abide by, this **<Organization>** Acceptable Use Policy:

_____ Date _____

Remote and Mobile Computing Policy

Instructions

This template is a starting point to enable you to create a Remote and Mobile Computing Policy tailored to meet the needs of your organization.

Perform a full document replacement of **<Organization>** with the proper name of your organization.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Contents

Purpose of the Policy

This policy provides specific information regarding remote and mobile computing mechanisms for information systems at **<Organization>**. The purpose of this policy is to ensure the security of remote working and mobile device use by employees of **<Organization>**.

Remote Information Processing refers to performing information processing activities in a remote location other than a **<Organization>** controlled facility. It includes the following sites:

- fixed locations (such as a residence)
- mobile locations (such as a hotel or airport)
- third-party locations (such as manufacturing partners, test facilities or contractor agencies)

Scope of the Policy

This policy applies to all client name employees, temporary staff, contractors and partners (“employees”). All employees are personally responsible for ensuring that they comply with this policy, and failure to do so may result in disciplinary action.

The policy applies to all mobile computing devices, whether personally owned or issued by **<Organization>**. This includes, but is not limited to smartphones, tablets, laptops and removable media devices.

Responsibility for Policy Implementation

The **<Organization>** Security Officer or other authorized representative shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

The **<Organization>** Security Officer or other authorized representative shall ensure compliance with the following standards:

Mobility

Theft Prevention

<Organization> Users are required to implement company-approved measures to prevent the theft of **<Organization>** owned/leased desktop and mobile computing devices

Types of Mobile Devices

Mobile computing devices include any computing device or media that is easily transportable outside of **<Organization>** premises, such as but not limited to the following:

- laptop computers
- USB mass storage devices
- mobile phones
- external hard drives
- optical media (CD/DVD/Blu-ray)

Accidental loss or theft incurs numerous hard and soft costs including the following:

- replacement cost of hardware
- re-licensing of software (operating systems/applications)
- incident reporting
- lost productivity
- exposure of proprietary information, perhaps to competitors
- exposure of sensitive employee information
- exposure of sensitive or confidential customer information
- potential federal, state and local fines associated with exposure of confidential employee or customer information
- damage to the reputation, brand, and market share of **<Organization>**
- misuse of **<Organization>** resources (for example, to commit a crime or harass **<Organization>** Users/customers)
- risk to **<Organization>** networks due to access to remote dialup scripts, email addresses, and passwords

Mobile Phones

Definitions

Mobile Phones – Any portable phone device (smart or otherwise) that, in addition to having the capability to make and receive phone calls, is also capable of receiving, transmitting and/or storing confidential information. Examples of mobile phones may include but are not limited to: cell phones and smartphones.

Confidential Information – Any individual's Personally Identifiable Information (PII); financial, operating or other proprietary **<Organization>** information; and other **<Organization>** information that is confidential in nature (e.g. employee compensation, benefit and disciplinary records).

External Storage Devices – any device that connects to an external interface of a computer, or to which data can be transferred. This including, but is not limited to USB, eSata, Firewire, Bluetooth, and wireless devices.

Remote Access – any network access that uses any network that is not owned and controlled by **<Organization>** as part of the connection. This includes home networks and public networks, as defined below.

Public Networks – any network that is located in a public location and allows patrons, customers, or other, non- authenticated users to connect to the network.

Mobile Phone Usage Standards and Policy

Only **<Organization>** mobile phones are permitted for conducting business requiring the use of a mobile phone. The use of a personal mobile phone for conducting <Organization> business is strictly prohibited unless the use of a personal mobile phone has been approved by an employee's leader.

General Provisions

Mobile Computing

<Organization> computer equipment security requirements are in effect for all mobile devices. These requirements include, but are not limited to:

- Strong authentication using password, PIN and/or biometric security. Mobile devices must be password protected in accordance with **<Organization>**'s Acceptable Use Policy.
- Prohibition of installing malicious programs, unauthorized software or tools onto mobile devices where such software and information can directly interact with **<Organization>** information stored on the mobile device.
- Prohibition of modifying configuration settings, disabling or removing malware protection, automatic update functions or other software on mobile devices.
- Remote locking and wipe functionality should be configured and enabled on mobile devices where available.
- Keep your mobile phone in a secure location when not in use and never leave it unattended.
- Install Apps only from trusted sources.
- Employees must not use instant messaging services to conduct business.
- Back up your data.
- Keep your system updated.
- Do not hack (jail-break, root) your device.
- Remember to log out of banking and shopping sites.
- Turn off Wi-Fi and Bluetooth services when not in use.
- Avoid sending personal information via Text or Email.
- Be careful what you click.
- Do not send confidential data over insecure (HTTP) connections.
- Do not connect to company resources from public networks (coffee shops, restaurants, libraries, airports, etc.).
- All laptops must have full hard disk encryption software switched on. The keys must be stored securely.
- Employees must only use a secure file-sharing site and application to securely access, share and save information.

Mobile Data

Stored Data

Appropriate measures to protect Data stored on remote or mobile devices must be implemented.

Precautions for Data Protection

Precautions to protect the data must apply regardless of the following:

- storage media on which information is recorded
- locations where the information is stored
- systems used to process the information
- individuals who have access to the information
- processes by which the information is handled

Locations

<Organization> Users shall use approved connection methods only when connecting from remote locations, including home networks, hotels, and public networks.

Minimizing Data Storage
Minimizing data storage on mobile devices will minimize the risk to data loss.

Remote Access Restrictions
<Organization> reserves the right to restrict, prevent, or otherwise control remote access to its network if <Organization> believes that such remote access is not being used in accordance with this directive, any directive, or supporting documents, or is otherwise detrimental to the interests of **<Organization>**.

Approved Hardware and Software
Hardware and software configurations for remote access computers must meet the same requirements as set out for equipment used on **<Organization>** premises. In particular, hardware and/or software that do not meet **<Organization>** business requirements must not be installed. Any workstation, either laptop or desktop, with non-approved hardware/software configurations must not connect to **<Organization>** networks.

Security Breach
Any suspected security breach relating to remote access must be immediately reported to a **<Organization>** leader.

Remote Access

Access to Remote Information Processing Facilities
Access to any remote information processing facilities must be through VPN and in conformance with **<Organization>** policies.

VPN Cryptography
Remote access VPN must employ cryptography which is in conformance with good computing practices.

Remote Access Logging
Remote access connection activity must be logged and have an audit trail. This is necessary for the security of **<Organization>** networks.

Additional Restrictions

[Instructions: Use this section to add policy provisions specific to your organization. Some examples of additional restrictions are shown below. Delete any items that do not apply to your desired policy and add any others that are appropriate.]

Allowed Devices
Only the following types of mobile devices shall be connected to **<Organization>** networks:

- List specific types, brands, models, etc. that should be allowed. Examples would be IOS devices only, laptops only, etc.
- Devices that have been approved by <Organization>'s Security Team

The following types of devices shall not be connected to any **<Organization>** network:

- List any types of devices that you do NOT want to allow to connect. Examples might be USB storage devices, Android devices, etc.

Allowed connection methods
Mobile devices connecting to **<Organization>** networks shall use the following connection methods only:

- List specific connection methods that you want to allow. If you wish to restrict connections to a specific VPN or remote access application, you can list it here.
- If you email service supports plain-text email (a dangerous practice in any case), you might want to prohibit its use.

Data storage restrictions
The following data types shall not be stored on mobile devices:

- List any specific types of data that you do not want users to store on mobile devices. This may include patient records, client lists, financial records, etc.

Mobile Device Management
All mobile devices connecting to **<Organization>** networks shall have **<Organization>**'s Mobile Device Management (MDM) software installed. Mobile devices shall be subject to the following restrictions:

Devices with operating system modifications (e.g. "rooted" or "jail-broken" devices) shall not be allowed to connect.

All devices shall have the following applications installed:

- List applications that are required.
- Any devices with the following applications installed shall not be connected to any **<Organization>** network. If found on a device, these applications may be remotely uninstalled.
- Device location may be tracked by **<Organization>** via the device's Global Positioning System (GPS) feature. Disabling the GPS feature is prohibited.
- You must immediately report any device that has been lost, stolen, misplaced, or is no longer under your direct control
- If a device is lost or stolen, data may be remotely deleted from the device. This may include any personal data that has been stored on the device.

Exceptions

[Instructions: Add any exceptions to the policy that you may want to include here. For example, certain persons or departments may be exempt from certain provisions.]

Implementation

[Instructions: Use this section to refer to any additional informational or procedural documents required for proper implementation of the policy. For example, there may be a "how-to" document describing the process for connecting to remotely to local resources via a VPN connection, etc.]

Note

Non-digital **<Organization>** information should only be taken off-site when necessary and must be subject to the same considerations as digital information.

Creating an Information Systems Disaster Recovery and Business Continuity Plan

This guide is intended to assist you in creating an Information Systems Disaster Recovery and Business Continuity Plan by providing the necessary background and context. An Information Systems Disaster Recovery and Business Continuity Plan should be part of your overall Disaster Recovery and Business Continuity Master Plan. The Master Plan will address all of the systems and resources required to operate your business in the event of a disaster or under other adverse conditions that would prevent normal business operations.

1. **The role of the Information Systems Disaster Recovery and Business Continuity Plan:**

   a. Every organization needs a comprehensive Business Continuity Plan that identifies which systems are critical for core business operations and describes the processes by which those systems will be sustained or recovered in a variety of circumstances. Those circumstances include disasters, but also include other planned and unplanned events, such as the departure or death of key personnel. A comprehensive Business Continuity Plan is very broad in scope and includes planning for financial systems, human resources, and all of the physical systems and infrastructure required to support business operations.

   b. The scope of this Information Systems Business Continuity Plan is restricted to those processes required to recover “information systems”. Information systems include the hardware, software, power and communications systems required to support and process the data required for core business operations.

2. **You also need a Data Backup and Disaster Recovery Plan:**

   a. This Information Systems Business Continuity Plan does not specifically address the recovery of business data. In many cases, your system recovery process will include data recovery in the restore points. If not, you MUST have a Data Backup and Disaster Recovery plan that documents the process for recovering data.

3. **Identifying the business mission-critical systems.**

   a. In a disaster, it may not be possible to restore all information systems within a timeframe that will prevent adverse impacts on operations. You must identify those systems that are most critical and must be recovered first. Make sure you include system dependencies, such as power, local network resources, and external connections.

4. **Identifying external service dependencies:**

   a. Power:

      1. For short-term power disruptions, are all servers and network devices protected by an Uninterruptable Power Supply (UPS). The primary purpose of a UPS is not to provide backup power for operations, although some UPS systems may do so. The primary purpose of a UPS system is to provide power to servers and storage devices for a time sufficient to allow proper shutdown of these devices. The UPS must be configured to signal devices that primary power has been lost and to initiate the shutdown sequence. Failure to allow proper shutdown greatly increases the risk of data loss or corruption. When installing UPS devices, consider:

         1. What is the expected run time for full operations?
         2. Do all servers receive shutdown commands from UPS units with sufficient time to ensure proper shutdown?
         3. Do servers and storage devices receive shutdown signals with enough remaining power capacity to ensure adequate time for a proper shutdown?

      2. For extended power outages, are there provisions for on-site power generation?

         1. If there is on-site power generation, what is the expected run time, based on the amount of fuel kept on hand?

   b. External network connections: If external network (Internet) connections are required for minimal business operations:

      1. Are redundant external network connections with different Internet Service Providers in place? ii. Does each of these connections provide adequate capacity for minimal business operations?

5. **Identifying the hardware on which recovered system will run (recovery hardware):**

   a. System recovery on the local network:

      1. How will external service dependencies be addressed?

   b. System recovery to a remote location

      1. How will external system dependencies be addressed?

         1. Are these services in place?
         2. Has the time required to install services been accounted for?

2. Is the hardware required for recovery installed at the remote site?
3. Is the software required for recovery installed and up to date?
4. Has the time required to update applications and data been accounted for?
5. How will users connect to the necessary resources?

c. System recovery to a data center location with company-supplied hardware (co-location)

1. Is the hardware required for recovery installed?
2. Is the software required for recovery installed and up to date?
3. Has the time required to update applications and data been accounted for?
4. How will users connect to the necessary resources?

d. Recovery to a public or private “cloud location”

1. Have the virtual machines and any necessary supporting infrastructure been created in advance?
2. Has the time required to update applications and data been accounted for?
3. How will users connect to the necessary resources?

6. **Recovery Service Level:**

a. At what capacity must these systems be recovered in order to maintain the minimum required functionality?

1. It may not be necessary, or possible, to recover systems at 100% capacity in a disaster. What are the minimum requirements for supporting critical business operations in a disaster? This is the Recovery Service Level, or RSL.

b. Outline the plan for ensuring that adequate resources will be available to meet the RSL.

7. **Maximum Tolerable Downtime:**

a. How long can these systems be down before business operations are adversely affected? This is the Maximum Tolerable Downtime.

8. **Recovery Time Objective:**

a. Analyze the system dependencies to determine which systems are most critical and which system depend on other systems for proper operation.

1. What is the maximum amount of time each system can be non-operational before business operations are adversely effected?
2. Can all critical systems be recovered in parallel, or must some systems be fully recovered before the recovery of other systems can begin (sequential recovery). The time required to recover all system to the Recovery Service Level is the Recovery Time Objective?

b. Outline the plan for ensuring that the RTO will be met

1. Where will the systems be recovered (list the devices and the process that will be used)?

9. **Restore Point Objective:**

   a. How much data can be lost?

      1. When systems fail, a certain amount of data loss is usually expected. The expected loss will be the data that has been entered into, or processed by, the system since the last “restore point”. Your backup software must create reliable restore points that preserve the integrity of all data. The frequency at which these restore points are created is the Restore Point Objective.

   b. Outline the plan for ensuring that the Recovery Point Objective will be met.

10. **System Recovery Initiation:**

   a. The Recovery Time Objective must be less than the Maximum Tolerable Downtime.
   b. System recovery must be initiated when the Actual Downtime (measured from when systems became non-operational) + the Recovery Time Objective = Maximum Tolerable Downtime.
   c. System recovery should begin XX hours after systems become non-operational.

11. **System recovery testing:**

   a. At what intervals will the following systems / processes be tested?

      1. Uninterruptable Power Supplies – network operations and device shutdown.
      2. Power generation systems.
      3. Individual server restore points.
      4. Full system recovery.

Information System Disaster Recovery and Business Continuity Plan

[Instructions: Below is an example of a typical system recovery plan for a system named “Primary Business Application”. This example plan is for the local recovery of the Primary Business Application within 4 hours with a maximum data loss of 1 hour. In the event of a disaster that renders the entire network unusable (such as a fire, flood, or extended power outage), the plan also provides for off-site recovery of the system in the outsourced IT service provider’s data center within 8 hours with a maximum data loss of 4 hours. Your recovery plan may not have the same requirements and may be more or less complex. You may need multiple business continuity plans for different systems. Below the example is a recovery plan template that you can copy. For more information, please refer to the accompanying guide Creating an Information Systems Disaster Recovery and Business Continuity Plan].

System Recovery Plan: Primary Business Application Name of Data Set	
Who is Responsible for configuration and management of recovery software and hardware?	IT Systems Inc. Network Operation Center
Who is Responsible for monitoring production system and initiating recovery processes?	IT Systems Inc. Network Operation Center
Who is responsible for managing recovery process?	IT Systems Inc. Network Operation Center
What Business applications are supported by this system?	Primary Business Application
What hardware and software components are required for system operation?	Domain controller, SQL Server, virtual switch
What is the Recovery service level (RSL) for this system?	50%
What is the Maximum Tolerable Downtime (MTD) for this system?	4 hours for local recovery, 8 hours for cloud recovery
What is the Recovery Time Objective (RTO) for this system?	45 minutes for local recovery and 2 hours for cloud recovery
What is the Recovery Point Objective (RPO) for this system?	1 hour for local recovery and 4 hours for cloud recovery
What is the Recovery Initiation Point (RIP) (MTD – RTO = time to initiate recovery) for this system?	3 hours 15 minutes for local recovery and 6 hours for cloud recovery

Describe the plan details and how objectives will be met in the space below

IT Systems Inc. is an outsourced IT services provider that operates a Network Operations Center (NOC) and a data center. IT Systems Inc. is responsible for managing this system recovery plan and all recovery processes.

The Primary Business Application requires the availability of two Microsoft Windows servers and network connectivity. A Domain controller must be available, so users can authenticate to the Microsoft SQL server that hosts the application.
Backup and recovery software running on the two production servers replicates to virtual machine images of the servers which are running on a Backup and Recovery Device installed in the server room. These images are updated hourly.
These images are then replicated to the IT Services Inc. data center and updated every 4 hours.
The NOC receives notice when any component of the Primary Business Application System is not functioning as expected and initiates recovery as per the plan.
In the event that either or both servers have failed, but the local network is still operational, the recovery virtual machine image(s) will be connected to the network. Data loss could be as much as 1 hour. In the event that both servers have failed, the recovery images will be running at approximately 50% of production capacity. Users will access the application from the local network as they normally would.
In the event the entire network has failed, as a result of an extended power outage or a natural disaster, the virtual images of the two servers are brought online at the IT Services Inc. data center. These servers will be able to communicate through a virtual switch at the data center. Users will be able to connect to the Primary Business Application from any computer, using an IP address and instructions that will be posted on Disaster Recovery page of the company website. Users will be able to download and install the client application. Once the client application has been installed, all features of the Primary Business Application will be available and business operations can continue.

Information System Disaster Recovery and Business Continuity Policy

Instructions

This template is a starting point to enable you to create an Information Systems Business Continuity Policy tailored to meet the needs of your organization.

This policy is intended to address business continuity for information systems only and should be part of a comprehensive Business Continuity Policy that addresses all of the business functions necessary for the continued effective operation of your organization.

Information systems recovery may, or may not, provide adequate recovery of the data sets required for business operations. Whether or not data recovery is included in information systems recovery processes, a separate Data Backup and Disaster

Recovery plan is required in order to ensure that critical business data is protected from all threats.

Please refer to the accompanying guide Creating an Information Systems Disaster Recovery and Business Continuity Plan for background and general information about information systems business continuity planning.

Perform a full document replacement of **<Organization>** with the proper name of your organization.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Contents

Purpose of the Policy

The purpose of this policy is to establish processes to ensure the availability of all information systems required for essential business operations in the event of an equipment failure, service disruption, or a loss of operational capacity resulting from a fire or natural disaster.

Scope of the Policy

This policy applies to all **<Organization>** devices, employees, and contractors. All employees and contractors with access to **<Organization>** computing devices or information systems shall comply with this policy as it applies to their job duties.

Definitions

Information system is defined as a system that is required to process information used in business operations. An information system includes all of the hardware, operating system software, application software, network connections, and external services required for proper operation.

Business mission-critical system is defined as an information system that is required to support essential business functions during both normal operations and during a disaster or other event that may limit the organization's capacity to conduct normal operations. Some business functions may not be mission-critical if loss of these system functionality does not adversely affect the organization's ability to conduct essential business operations.

Off-site location is defined as a physical location that is geographically distant from the production location such that no single weather-related or other disaster would be likely to affect both locations.

Public or Private "cloud" is defined as a collection of hardware and software that is located in a secure location with redundant systems for power and Internet connectivity. Public clouds are multi-tenant data centers where computing infrastructure can be purchased at a required capacity, on either a temporary or permanent basis. Private clouds are owned by the organization or an affiliate and are not available to the general public.

External services are defined as services that are provided by an external provider, such as a power company or Internet Service Provider (ISP).

Restore Service Level (RSL) is defined as the required capacity of an information system for minimal or interim operations. If a system operating at 50% of its normal operating capacity is adequate to support minimal business operations during a failure or disaster event, then the RSL is 50%.

Maximum Tolerable Downtime (MTD) is defined as the maximum amount of time that an information system can remain non-functional before business operations are adversely affect.

Restore Time Objective (RTO) is defined as the time required to restore an information system from its maintained (backup) state to the Restore Service Level, establish connectivity, and make it available for business operations.

Restore Point Objective (RPO) is defined as the maximum amount of data loss that can be tolerated in terms of time. If the RPO is 1 hour, then restore points must be created on an hourly basis.

Recovery Initiation Point (RIP) is the time when recovery should be initiated. This typically occurs when the time since system failure plus the Recovery Time Objective is equal to the Maximum Tolerable Downtime. For example, if the Recovery time objective is 1 hour and the Maximum Tolerable Downtime is 5 hours, recovery should be initiated 4 hours after system failure. RIP can also be expressed as MTD minus RTO.

Responsibility for Policy Implementation

The **<Organization>** Security Officer or other authorized representative shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

This Policy works in conjunction with the Creating an *Information Security Disaster Recovery and Business Continuity Plan*. The **<Organization>** Security Officer or other authorized representative shall ensure compliance with the following standards:

1. Data Backup and Disaster Recovery Plan: The Security Office shall create, test and maintain a Data Backup and Disaster Recovery Plan to ensure proper backup and recovery of critical business data. This is required even if data recovery is included in the Information Systems Disaster Recovery and Business Continuity Plan. The Data Backup and Disaster Recovery Plan may refer to the Information Systems Disaster Recovery and Business Continuity plan as part of one or more Data Backup Plans.
2. A Recovery Time Objective (RTO) must be determined for critical systems. System dependencies must also be determined and considered. The RTOs must always be less than the maximum tolerable downtime. System RTOs must be documented and logged to inform future Business Continuity Plan tests.
3. All servers and data storage devices must be protected by Uninterruptable Power Supply (UPS) devices to protect
4. against power fluctuations and short-term disruptions.
5. All UPS devices shall be configured to send shutdown signals to all servers and data storage devices, allowing sufficient time to allow for proper shutdown.
6. Recovery hardware should be identified and documented in an asset register. This should include all local network hardware, remote location hardware, remote location with company owned hardware (co-location) and public or private cloud storage locations on which system recovery will run.
7. Where possible, external services should be redundant (e.g. multiple ISP connections, on-site power generators, etc.)
8. Testing of the Disaster Recovery and Business Continuity Plan should occur twice a year. The test should be fully documented in a post-test report, and future tests demonstrably informed by the previous tests activities.

Communication of the Policy

The **<Organization>** Security Officer shall communicate this policy to appropriate individuals as necessary to ensure proper implementation.

Policy Violations and Non-compliance

Intentional violations of this policy shall subject the violator to appropriate sanctions. These sanctions may include suspension or dismissal.

Policy non-compliance shall result in a written warning for the first violation. Subsequent sanctions will be at the discretion of the Security Officer.

Creating a Data Backup and Disaster Recovery Plan

This guide is intended to assist you in creating a Data Backup and Disaster Recovery Plan by providing the necessary background and context. A Data Backup and Disaster Recovery plan should be part of your overall Disaster Recovery and Business Continuity Master Plan. The Master Plan will address all of the systems and resources required to operate your business in the event of a disaster or under other adverse conditions that would prevent normal business operations.

1. **The critical role of data in business operations:**

   a. Every organization needs a comprehensive Disaster Recovery Plan that:

      1. Identifies the critical business functions that could be affected by a disaster.
      2. dentifies the resources that must be preserved or recovered in order to restore business operations after a disaster.
      3. Documents action plans for how those resources will be restored.

   b. A comprehensive Disaster Recovery Plan includes planning for areas including human resources, physical resources, information resources, and external systems, such as power and communication channels.
   c. Protecting business data is second in importance only to protecting life. Buildings, fixtures, machinery, computer hard- ware, and computer software can all be replaced. Data cannot, and thus requires special protections.
   d. This is not a comprehensive Disaster Recovery Plan. The scope of this plan is restricted to those processes required to recover “electronic data” which includes any documents or other records that are stored in an electronic form and are required for effective business operations.
   e. Although this Data Backup and Disaster Recovery Plan pertains to electronic data, some organizations also maintain physical records. These are generally paper documents. Physical documents are beyond the scope of this Plan.

If physical records are important to your organization, a process for preserving them should be documented in a separate policy.

1. By definition, there can be only one “original” document. If it is destroyed, recovery is not possible. However, it may be possible to create physical copies for disaster recovery purposes.
2. Electronic copies of physical records are considered electronic data and would be included in the Data Backup and Disaster Recovery Plan.

2. **All digital copies of electronic data are identical:** Electronic data that is digitally encoded can be duplicated and any number of copies may exist. All copies are identical and there is no differentiation for any legal or other purpose between existing copies.

3. **Risks to electronic data:** Threats to electronic data can be placed into 3 categories:

   a. Data confidentiality – data confidentiality is violated when information is viewed or accessed by a person or process that is not authorized to do so.
   b. Data integrity – Data integrity is violated when the data is altered by a person or process that is not authorized to do so.
   c. Data Availability – Data availability is violated when persons or processes that are authorized to view or access data cannot do so when required.

4. **The role of disaster recovery in a business risk management plan:**

   a. Your organization should complete a risk assessment and create a Cyber Risk Management Plan to address all threats to the confidentiality, integrity, and availability of electronic data. This Backup and Disaster Recovery Plan is one component of Cyber Risk Management Plan.
   b. This Disaster Recovery Plan is primarily intended to address data availability in the event of a natural disaster or other unanticipated failure. Your organization needs to create other policies, procedures and controls that address data confidentiality and data integrity, as well as other business risks.
   c. Although disaster recovery addresses risks to data availability, the recovery processes must be designed and implemented in such a way that data confidentiality and data integrity are not compromised.
   d. Data is often unusable unless the systems required to process the data are available. If line-of-business applications or systems are required to make the data usable, you must also create an Information Systems Business Continuity Plan.

5. **Data backup – the 3-2-1-A rule:**

   a. Electronic data can be damaged or lost as a result of human error, external events, or device failure. The MINIMUM requirements to protect data from these threats are:

      1. AT LEAST 3 updated copies of the data must be maintained.
      2. Copies must exist on AT LEAST 2 physical devices in order to protect against device failure
      3. AT LEAST 1 copy must be maintained “off-site”. That is, in a geographically separate location that would not be affected by a fire or weather affecting the location where other copies are maintained.
      4. Backup processes must be executed Automatically. If the backup process depends upon someone remembering to initiate backups at the proper times, there will inevitably be failures.

1. Automatic backup processes should, at a minimum, include notification of failures.
2. There some failures that will include failure of the notification system. Therefore, monitoring for expected backup "success" notifications should be implemented whenever possible.

6. **Defining data sets:**

a. Determine which folders contain data that must be backed up. This must include any files or documents that are created by users or by applications.
b. Folders with the same backup and recovery requirements should be combined into data sets. The data sets that are directly accessed by users or applications are the "production data sets". Backup copies of the production data sets are "backup data sets".
c. Database files:

1. Unlike most documents, database files are constantly changing. Maintaining the integrity of database files requires special processes. Therefore, database files should be identified separately to ensure that the proper processes are applied. In many cases, proper database file backup can only be achieved by using the vendor's backup process. The resulting files should then be backed up as part of the regular backup routine.

7. **Data backup confidentiality and integrity controls:**

a. Confidentiality controls:

1. When confidential data is backed up, the same access controls that apply to the production data sets should be applied to the backup data sets
2. Encryption of backup sets: Most backup software provides an option to encrypt the backup data sets. When backing up confidential data, encrypting is generally best practice. However, there must also be a process for securely storing the encryption keys (usually a password) and ensuring that it is available and can be applied during the restore process. A lost encryption key will generally render a backup data set useless.

b. Integrity

1. File integrity controls (checksums, hashes, etc.) ii. Database integrity controls

8. **Data backup vs. data replication:**

a. Data replication and data backup have different purposes. Proper protection of your data may or may not require replication, but will always require data backup.
b. Data replication is essentially creating a "mirror" of the data. Changes made to the production data are replicated to the "mirror" at specified intervals, or in as nearly to real time as possible.

1. Replication is used to maintain a copy of the data set in the most current version possible.
2. Replication is NOT a substitute for data backup. Events that would damage the production data set, such as file corruption and inadvertent deletions, are typically mirrored in the replicated data as well. Replication does not provide an option for restoring data to a previous known state.

c. Data backup is used to create the ability to restore data to a previous state. A data backup set is a point in time "snap- shot" of the data. The backup data set is not affected by any subsequent changes.

9. **Backup types:**

a. Backups are generally classified as full, differential, or incremental. Backups are also either done at the file level or at the storage device "block level". The type of backup determines the time required to complete the backup and the storage requirements. Some backup types depend on a "backup chain". If any link in the chain is broken (e.g. a file is corrupt), then all subsequent backup points in that chain are unusable. Details regarding the most effective use of these backup types are beyond the scope of this document. The person(s) responsible for planning and implementing the backup plans MUST have a thorough understanding of these backup types and how to implement them.

10. **Backup data set locations:**

a. As per the 3-2-1-A rule described above, critical business production data sets must ALWAYS be copied to AT LEAST 2 locations, with one of them being "off-site".
b. As per the "Backup data confidentiality and integrity controls section above, access to ALL data backup locations must be controlled.
c. When backup sets are being transmitted over local or wide-area network connections, consider:

1. Security. Use secure, encrypted connections when transmitting confidential information.
2. Bandwidth requirements. In order to minimize the amount of bandwidth consumed by the transfer of backup data sets, it may be possible to:

1. Implement backup methods that use or generate smaller backup data sets, such as incremental and/or block-level backups.
2. Save backup sets to local disks during business operating hours and then copy those backup data sets to off-site locations over slower wide-area connections during non-business hours.
3. In either case, the increased risks of data loss should be balanced against the need to conserve bandwidth.

11. **Data backup interval:**

a. The interval at which backups are conducted is determined by the amount of data loss that is tolerable. It is always reasonable to assume that all data entered, updated, or processed since the most recent backup will be lost. Thus, if the maximum tolerable data loss is 1 hour, backups must be conducted on an hourly basis.

12. **Data retention policies:**

a. Each data set must have an associated Data Retention Policy. This policy documents the number of restore points that must be maintained. In order to address storage space limitations, these restore points are typically consolidated after a specified period of time. A typical data retention policy would look something like this:

1. Hourly restore points are retained for XX days, and are then consolidated into a single restore point for each day.
2. Daily restore are retained for XX days, and are then consolidated into single weekly restore point.

3. Weekly restore points are retained for XX weeks and are then consolidated into monthly restore points.
4. Monthly restore points are retained for XX months

b. The data retention policy should be determined by the business needs for access to data.

13. **Data restore testing:**

a. File restore testing must be done periodically to ensure that the process can be completed successfully. After all, what your business needs is really a data RESTORE solution, rather than a data backup solution.
b. Database testing must be done as a separate process. Simply restoring a database file does not ensure its internal integrity. It is necessary to mount the database file in the application that uses it in order to test functionality.

Data Backup and Disaster Recovery Policy

Instructions

This template is a starting point to enable you to create a Data Backup and Disaster Recovery Policy tailored to meet the needs of your organization.

Please refer to the accompanying guide Creating a Data Backup and Disaster Recovery Plan for background and general information about data backup and disaster recovery planning.

Perform a full document replacement of **<Organization>** with the proper name of your organization.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Contents

Purpose of the Policy

The purpose of this policy is to establish processes that will ensure the availability of critical information in the event of inadvertent deletion or corruption of data, device failure, business interruption, or business disruption resulting from a fire or natural disaster.

Scope of the Policy

This policy applies to all **<Organization>** devices, employees, and contractors. All employees and contractors with access to **<Organization>** computing devices or information systems shall comply with this policy as it applies to their job duties.

Definitions

Data replication is defined as a process to replicate or "mirror" the most current version of data to another location. Data replication is not the same as data backup.

Data backup is defined as a process of copying data to another location and creating "restore points" which can be used to restore data to a previous state.

Off-site location is defined as a physical location that is geographically distant from the production location such that no single weather-related or other disaster would be likely to affect both locations.

Retention policy is defined as a process for determining how long data restore points should be retained, and/or when they should be consolidated into less frequent restore points.

Data set is defined as a collection of data folders with similar backup and retention requirements that are grouped together and are subject to the same data backup plan.

Data processing application is defined as the application that is required in order to process data and make it usable. In most cases, data is not usable unless the data processing application is available.

Backup application is defined as the software application that is used to perform backup operations.

Failure notification is defined as a process whereby the backup application generates and sends a notification (usually via email) that a backup process has failed. The absence of a failure notification does not ensure backup success, since a backup application that is not running or has failed may not be able to send failure notifications.

Success notification is defined as a process whereby the backup application generates and sends a notification (usually via email) that a backup process has succeeded. Success notifications can be monitored to ensure that the backup application is running and backups are being completed successfully.

PII (Personally Identifiable Information) is defined in NIST Special Publication 800-122 as any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

ePHI, or PHI (Protected Health Information) is Information in any format that identifies the individual, including demographic information collected from an individual that can reasonably be used to identify the individual. Additionally, PHI is information created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual. ePHI is PHI that is stored or transmitted in an electronic format.

Restore Point Objective (RPO) is defined as the maximum amount of data loss that can be tolerated in terms of time. If the RPO is 1 hour, then restore points must be created on an hourly basis.

Restore Time Objective (RTO) is defined as the time required to restore an information system from its maintained (backup) state to the Restore Service Level, establish connectivity, and make it available for business operations.

[Suggestion: RPOs and RTOs should be defined individually for critical systems and data, which should be logged in a documented backup schedule. If no specific definition has been applied, your organization should determine a default value based on the criticality of the data they handle, and provisions codified in relevant regulatory and legal frameworks that they oblige by.]

Responsibility for Policy Implementation

The **<Organization>** Security Officer or other authorized representative shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

This Policy works in conjunction with the Creating an *Information Security Disaster Recovery and Business Continuity Plan*. The **<Organization>** Security Officer or other authorized representative shall ensure compliance with the following standards:

1. Data backups:

    a. Critical systems and data must be backed up so that the minimum RPO and RTO can be met
    b. All ePHI and other critical business data shall be backed up on at least a daily basis. All ePHI and other critical business data shall be backed up to an off-site location on at least a daily basis.
    c. All backup copies of PII and ePHI shall be encrypted in accordance to **<Organization>**'s encryption policy and the relevant regulatory requirements of the jurisdiction that they operate in.
    d. The ability to restore data from backups shall be tested on a least a semi-annual basis.
    e. Data replication is not the same as data backup. A data backup plan must include the ability to restore data to a previous state.
    f. If data is backed up to the cloud, the cloud storage provider must have security, encryption and restore capabilities that mirror those outlined in this policy. These should be explicitly agreed upon in Service Level Agreements with the cloud storage provider prior to their use.
    g. Where data is hosted by third parties, or SaaS, the service agreement must contain a description of the backup and recovery objectives. These should be in line with **<Organization>**'s own backup and recovery objectives and periodically reviewed through vendor risk assessments.
    h. Where backup is to removeable media, it must be kept in a locked area with access restricted to only authorized individuals with a legitimate reason to access the data (e.g. authorized users within **<Organization>**'s IT department).

2. Data retention and versions:

    a. When ePHI or other critical business data is changed, a minimum of 5 previous versions shall be retained for a minimum of 30 days. Care should be taken to ensure the PII and ePHI is only pertaining to data covered within your jurisdiction, for example the Ontario PHIPA. If, for example, it involved date subjects residing within the EU, then the data would be subject to the data retention periods specified under the GDPR for special category personally identifiable information. In this instance, Article 5 (e) of the GDPR states “personal data shall be kept for no longer than is necessary for the purposes for which it is being processed”, of which a further process would have to be determined based off a data privacy impact assessment to determine a compliant retention schedule. N.B: If no EU resident data is processed for any client that this template is handed out to, please ignore this point.

3. Business continuity:

    a. The Security Office shall create and maintain a Business Continuity Plan that ensures the continued availability of the information systems required for business operations in the event of a business interruption caused by a service disruption (e.g. an extended power outage) or some other event.

4. Disaster Recovery:

    a. The Security Officer shall create and maintain a Disaster Recovery Plan that ensures the recovery of all resources required for business operations event of a disaster, such as a major equipment failure, a fire, or a natural disaster.

Communication of the Policy

The **<Organization>** Security Officer shall communicate this policy to appropriate individuals as necessary to ensure proper implementation.

Policy Violations and Non-compliance

Intentional violations of this policy shall subject the violator to appropriate sanctions. These sanctions may include suspension or dismissal.

Policy non-compliance shall result in a written warning for the first violation. Subsequent sanctions will be at the discretion of the Security Officer.

Backup Plan

[Instructions: You need a Backup Plan for each Data Set that you define. Below is an example backup plan for a data set named “Customer Database”. Below the example is a template that you can copy. For more information, please see the accompanying guide Creating a Data Backup and Disaster Recovery Plan].

Data Set: Customer Database

Local Backup		Off-Site Backup	
Person responsible for creating, maintaining, and monitoring this backup set	J. Smith	Person responsible for creating, maintaining, and monitoring this backup set	R. Jones
Frequency	Hourly	Frequency	Daily
Data processing application	Microsoft SQL Server	Application	Microsoft SQL Server
Backup application	My local backup application	Backup Application	My online backup application
Backup type	Incremental, with weekly full	Backup type	Incremental. 10 versions
retained			
Encrypted	Yes	Encrypted	Yes
Application is database- aware	Yes	Application is database- aware	No
Destination	Local NAS device	Destination	Online
Automatic	Yes	Automatic	Yes
Failure notification	Yes	Failure notification	Yes
Success notification	Yes, via control panel daily report	Success notification	No
Retention policy	Customer DB local retention policy	Retention policy	Customer DB online retention policy
Restore last tested	Sep 1, 2014	Restore last tested	Nov 5, 2014
Restore tested by	J. Smith	Restore tested by	R. Jones

Name of Data Set

Local Backup		Off-Site Backup	
Person responsible for creating, maintaining, and monitoring this backup set	J. Smith	Person responsible for creating, maintaining, and monitoring this backup set	R. Jones
Frequency	Hourly	Frequency	Daily
Data processing application	Microsoft SQL Server	Application	Microsoft SQL Server
Backup application	My local backup application	Backup Application	My online backup application
Backup type	Incremental, with weekly full	Backup type	Incremental. 10 versions
retained			
Encrypted	Yes	Encrypted	Yes
Application is database- aware	Yes	Application is database- aware	No
Destination	Local NAS device	Destination	Online
Automatic	Yes	Automatic	Yes
Failure notification	Yes	Failure notification	Yes
Success notification	Yes, via control panel daily report	Success notification	No
Retention policy	Customer DB local retention policy	Retention policy	Customer DB local retention policy
Restore last tested	Sep 1, 2014	Restore last tested	Nov 5, 2014
Restore tested by	J. Smith	Restore tested by	R. Jones