Information Classification and Handling Policy

|  |  |
| --- | --- |
| DOCUMENT CLASSIFICATION | FOUO |
| DOCUMENT REF |  |
| VERSION | 1 |
| DATED | 15 October 2024 |
| DOCUMENT AUTHOR | Kevin Bacon |
| DOCUMENT OWNER | CISO |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | REVISION AUTHOR | SUMMARY OF CHANGES |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution

|  |  |
| --- | --- |
| NAME | TITLE |
|  |  |
|  |  |
|  |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | POSITION | SIGNATURE | DATE |
| Gage Radtke | CEO |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Introduction 4](#_Toc42604085)

[2 **Information Classification…………………………………………………………………**5](#_Toc42604086)

[3 **Information Handling Procedures …………..……………………………………………**5](#_Toc42604086)

[4 **Security Awareness and Training ...………………………………………………………**6](#_Toc42604086)

[5 **5. Incident Response**……………………………………………………………………..**…**6](#_Toc42604086)

[6 **Compliance and Legal Requirements ……………………………………………………**6](#_Toc42604086)

[7 **Policy Review and Updates …………..……………………………………………………**6](#_Toc42604086)

**Information Classification and Handling Policy**

**1. Introduction**

This Information Classification and Handling Policy outlines the procedures for classifying, handling, and protecting sensitive information within the company. The goal of this policy is to ensure the confidentiality, integrity, and availability of our information assets.

Personal information is any information about any living, identifiable individual. The organization is legally responsible for this, and its storage, protection and use are governed by national and international law. Details of specific requirements for personal information can be found in the *Privacy and Personal Data Protection Policy*.

The organization maintains inventories of all-important information assets upon which it relies. However, Northwoods Naturals recognises that there are risks associated with employees, customers, contractors and other third parties accessing and handling information in order to conduct official organization business.

Northwoods Naturals has a responsibility to protect the information it holds and processes using controls appropriate to the sensitivity of the information involved.

Only by classifying information according to a documented scheme can the correct level of protection be applied. This procedure sets out the details of the scheme to be adopted and the criteria applied in deciding which level of protection to apply to any given information asset.

This control applies to all systems, people and processes that constitute the organization’s information systems, including board members, directors, employees, suppliers and other third parties who have access to [Organization Name] systems.

The following policies and procedures are relevant to this document:

* *Information Asset Inventory*
* *Information Labelling Procedure*
* *Access Control Policy*
* *Privacy and Personal Data Protection Policy*
* *Acceptable Use Policy*

**2. Information Classification**

The Northwoods Naturals information classification scheme requires information assets to be protectively marked into one of 3 classifications (excluding Public information which does not need to be marked). The way the document is handled, published, moved and stored will be dependent on this scheme.

Information will be classified into the following categories:

* **Level 0: Public:** Information that can be freely disclosed to the public.
* **Level 1: Internal (or FOUO):** Information that is confidential to the company and should not be shared with external parties without authorization.
* **Level 2: Confidential:** Information that is sensitive and requires a high level of protection. This may include customer data, financial information, and intellectual property.
* **Level 3: Highly Confidential:** Information that is extremely sensitive and requires the highest level of protection. This may include trade secrets, proprietary information, and personal data.

**3. Information Handling Procedures**

**3.1 Access Controls**

* Access to information will be restricted to authorized personnel on a need-to-know basis.
* Strong passwords and multi-factor authentication will be required to access sensitive systems.
* Role-based access controls will be implemented to limit access to specific information.

**3.2 Information Sharing**

* Information will only be shared with authorized individuals or organizations.
* When sharing information with external parties, appropriate security measures will be taken to protect the confidentiality and integrity of the information.

**3.3 Data Storage and Backup**

* Sensitive data will be stored on secure servers with appropriate access controls.
* Regular backups of critical systems and data will be performed.
* Backups will be stored securely and encrypted.

**3.4 Data Destruction**

* When information is no longer needed, it will be securely destroyed to prevent unauthorized access.
* Data destruction methods will comply with applicable laws and regulations.

**4. Security Awareness and Training**

* All employees will receive regular security awareness training.
* Training will cover topics such as password security, phishing attacks, and data protection.

**5. Incident Response**

* A comprehensive incident response plan will be in place to address security breaches and data loss.
* The incident response team will be responsible for investigating incidents, containing the damage, and restoring normal operations.

**6. Compliance and Legal Requirements**

* The company will comply with all applicable laws and regulations, including data privacy laws (e.g., GDPR, CCPA) and industry standards (e.g., PCI DSS).
* Regular security audits and assessments will be conducted to identify and address vulnerabilities.

**7. Policy Review and Updates**

This Information Classification and Handling Policy will be reviewed and updated annually or as needed to ensure its effectiveness.

By following this policy, the company can protect its valuable information assets and maintain the trust of its customers and partners.

**Access and Authentication Policy**

**Introduction**

A comprehensive Access and Authentication Policy is essential for safeguarding sensitive customer and company data in an e-commerce environment. This policy outlines the guidelines for accessing and authenticating users, minimizing the risk of unauthorized access and data breaches.

**Policy Statement**

The company is committed to protecting the confidentiality, integrity, and availability of its information assets. This policy establishes the standards and procedures for controlling access to systems and data, ensuring that only authorized individuals can access the appropriate resources.

**Scope**

This policy applies to all employees, contractors, and third-party vendors who have access to the company's information systems, networks, and data.

**Access Control**

1. **Principle of Least Privilege:**
   * Grant access to systems and data on a need-to-know basis.
   * Assign the minimum level of access required to perform job functions.
2. **Role-Based Access Control (RBAC):**
   * Define roles and assign appropriate permissions to each role.
   * Regularly review and update role assignments.
3. **Password Policy:**
   * Enforce strong password requirements, including:
     + A minimum length of [number] characters
     + A combination of uppercase and lowercase letters, numbers, and special characters
     + Password expiration and rotation
     + Password complexity rules
   * Prohibit password reuse
4. **Multi-Factor Authentication (MFA):**
   * Implement MFA for all privileged accounts and sensitive systems.
   * Consider using a combination of:
     + Something you know (password)
     + Something you have (security token)
     + Something you are (biometric authentication)
5. **Session Timeouts:**
   * Set appropriate session timeout durations for all user sessions.
   * Automatically log users out after a period of inactivity.
6. **Access Reviews:**
   * Conduct regular access reviews to ensure that permissions are still valid and necessary.
   * Revoke access for terminated employees or contractors promptly.

**Authentication**

1. **Strong Authentication Mechanisms:**
   * Utilize strong authentication methods, such as:
     + Password-based authentication with strong password policies
     + Biometric authentication (fingerprint, facial recognition)
     + Token-based authentication (hardware or software tokens)
2. **Secure Authentication Protocols:**
   * Employ secure authentication protocols like OAuth, OpenID Connect, or SAML.
3. **Regular Password Changes:**
   * Enforce regular password changes to minimize the risk of unauthorized access.

**Monitoring and Logging**

1. **System and Network Monitoring:**
   * Implement robust system and network monitoring tools to detect and respond to security threats.
2. **Security Information and Event Management (SIEM):**
   * Utilize SIEM solutions to collect, analyze, and correlate security event logs.
3. **Intrusion Detection Systems (IDS):**
   * Deploy IDS to identify and respond to unauthorized access attempts.
4. **Access Logs:**
   * Maintain detailed access logs to track user activities and identify anomalies.

**Incident Response**

1. **Incident Response Plan:**
   * Develop and maintain a comprehensive incident response plan to address security breaches.
2. **Incident Reporting:**
   * Establish clear procedures for reporting security incidents.
3. **Incident Investigation:**
   * Conduct thorough investigations to determine the root cause of security incidents.
4. **Remediation and Recovery:**
   * Implement effective remediation measures to mitigate risks and restore system integrity.

**Awareness and Training**

1. **Security Awareness Training:**
   * Provide regular security awareness training to all employees to educate them about security best practices.
2. **Phishing Awareness Training:**
   * Conduct phishing awareness training to help employees identify and avoid phishing attacks.

**Compliance**

1. **Industry Standards and Regulations:**
   * Adhere to relevant industry standards (e.g., PCI DSS, HIPAA) and regulatory requirements (e.g., GDPR, CCPA).
2. **Regular Audits and Assessments:**
   * Conduct regular security audits and assessments to identify and address vulnerabilities.

**Conclusion**

By implementing this Access and Authentication Policy, the company can significantly enhance its security posture and protect its valuable assets. Regular review and updates to this policy are essential to ensure its effectiveness in the face of evolving threats.

**Network Security Policy**

**1. Introduction**

This Network Security Policy outlines the guidelines and procedures for securing the company's network infrastructure, systems, and data. The goal of this policy is to protect the confidentiality, integrity, and availability of our network resources.

**2. Network Security Standards**

* **Strong Password Policy:** Enforce strong password requirements, including a minimum length, a combination of uppercase and lowercase letters, numbers, and special characters, and regular password changes.
* **Multi-Factor Authentication (MFA):** Implement MFA for all privileged accounts and sensitive systems to enhance security.
* **Secure Network Configuration:** Configure network devices (routers, switches, firewalls) with secure default settings and strong access controls.
* **Regular Security Patching:** Keep all network devices, servers, and workstations up-to-date with the latest security patches and software updates.
* **Intrusion Detection and Prevention Systems (IDS/IPS):** Deploy IDS/IPS systems to monitor network traffic for signs of malicious activity and block potential threats.
* **Firewall Protection:** Implement robust firewall protection to control network traffic and prevent unauthorized access.
* **Secure Remote Access:** Use strong authentication and encryption for remote access to the network.
* **Data Encryption:** Encrypt sensitive data both at rest and in transit to protect it from unauthorized access.
* **Network Segmentation:** Segment the network into different zones to limit the impact of potential security breaches.
* **Regular Security Audits and Penetration Testing:** Conduct regular security audits and penetration testing to identify and address vulnerabilities.

**3. Network Access Control**

* **Access Control Lists (ACLs):** Use ACLs to restrict network access to authorized users and devices.
* **Port Security:** Configure port security on network switches to limit the number of devices that can connect to a specific port.
* **Network Access Control (NAC):** Implement NAC solutions to enforce security policies and prevent unauthorized devices from accessing the network.

**4. Incident Response**

* **Incident Response Plan:** Develop and maintain a comprehensive incident response plan to address security incidents.
* **Incident Reporting:** Establish clear procedures for reporting security incidents.
* **Incident Investigation:** Conduct thorough investigations to determine the root cause of security incidents.
* **Remediation and Recovery:** Implement effective remediation measures to mitigate risks and restore system integrity.

**5. Employee Awareness and Training**

* **Security Awareness Training:** Provide regular security awareness training to all employees to educate them about network security best practices.
* **Phishing Awareness Training:** Conduct phishing awareness training to help employees identify and avoid phishing attacks.

**6. Compliance and Legal Requirements**

* **Industry Standards and Regulations:** Adhere to relevant industry standards (e.g., PCI DSS, HIPAA) and regulatory requirements (e.g., GDPR, CCPA).
* **Regular Audits and Assessments:** Conduct regular security audits and assessments to identify and address vulnerabilities.

By following this Network Security Policy, the company can significantly enhance its security posture and protect its valuable network resources. Regular review and updates to this policy are essential to ensure its effectiveness in the face of evolving threats.

Incident Response Policy

1. Introduction

This Incident Response Policy outlines the procedures and guidelines to be followed in the event of a security incident that could potentially impact the company's systems, networks, data, or reputation. The goal of this policy is to minimize the impact of incidents, protect sensitive information, and restore normal operations as quickly as possible.

2. Incident Definition

An incident is defined as any event or series of events that could potentially compromise the confidentiality, integrity, or availability of the company's information assets. This includes, but is not limited to:

• Security breaches

• Unauthorized access

• Malware infections

• Data breaches

• Denial-of-service attacks

• System failures

• Natural disasters

3. Incident Response Team

An Incident Response Team (IRT) will be established to coordinate the response to security incidents. The IRT will consist of representatives from various departments, including:

• Information Technology

• Security

• Legal

• Public Relations

• Operations

4. Incident Response Procedures

4.1 Incident Detection and Reporting

• Employees are encouraged to report any suspected security incidents to the IT department or the IRT.

• Automated systems and tools will be used to monitor networks and systems for signs of intrusion or anomalies.

• Incident detection and reporting procedures will be documented and regularly reviewed.

4.2 Incident Assessment

• Upon detection of an incident, the IRT will be activated to assess the situation.

• The IRT will determine the scope, severity, and potential impact of the incident.

• A preliminary incident report will be created to document the initial findings.

4.3 Incident Containment

• The IRT will take immediate steps to contain the incident and prevent further damage.

• This may involve isolating affected systems, blocking network traffic, or implementing other security measures.

4.4 Incident Eradication

• Once the incident is contained, the IRT will work to eradicate the threat.

• This may involve removing malware, patching vulnerabilities, or restoring compromised systems.

4.5 Incident Recovery

• The IRT will coordinate the recovery of affected systems and data.

• This may involve restoring backups, reconfiguring systems, and retraining users.

4.6 Post-Incident Analysis

• After the incident is resolved, the IRT will conduct a thorough analysis to identify the root cause and lessons learned.

• A post-incident report will be created to document the findings and recommendations.

• Corrective actions will be implemented to prevent similar incidents from occurring in the future.

5. Communication and Notification

• The IRT will communicate with key stakeholders, including management, employees, and customers, as needed.

• A communication plan will be developed to ensure timely and accurate information is disseminated.

• In the event of a significant data breach, the company will comply with applicable laws and regulations regarding notification requirements.

6. Regular Review and Updates

This Incident Response Policy will be reviewed and updated annually or as needed to reflect changes in the company's security environment.

By following this Incident Response Policy, the company can effectively respond to security incidents, minimize damage, and protect its reputation.

**Business Continuity and Disaster Recovery Policy**

**1. Introduction**

This Business Continuity and Disaster Recovery (BCDR) Policy outlines the strategies and procedures to ensure the continuity of business operations in the event of disruptions, such as natural disasters, cyberattacks, or system failures. The goal of this policy is to minimize business downtime, protect critical data, and maintain customer satisfaction.

**2. Business Impact Analysis (BIA)**

A comprehensive Business Impact Analysis (BIA) will be conducted to identify critical business functions, assess potential risks, and determine recovery time objectives (RTOs) and recovery point objectives (RPOs).

**3. Disaster Recovery Plan (DRP)**

A detailed Disaster Recovery Plan (DRP) will be developed to outline the steps to be taken in the event of a disaster. The DRP will include:

* **Incident Response Procedures:** Clear guidelines for detecting, reporting, and responding to incidents.
* **Data Backup and Recovery Procedures:** Regular backups of critical data, including system images, databases, and applications.
* **Disaster Recovery Site:** A designated off-site location for backup systems and data, which can be activated in case of a disaster.
* **Business Continuity Plan:** Strategies to maintain critical business functions during a disaster, such as remote work arrangements, alternative suppliers, and contingency plans.

**4. Technology Recovery**

* **Server and Network Recovery:** Procedures for restoring servers, network devices, and virtual infrastructure.
* **Data Recovery:** Procedures for recovering lost or corrupted data from backups.
* **Application Recovery:** Procedures for restoring critical applications and databases.

**5. Communication Plan**

* **Internal Communication:** A communication plan to inform employees about the incident and provide updates on recovery efforts.
* **External Communication:** A communication plan to inform customers, suppliers, and other stakeholders about any disruptions and the steps being taken to restore services.

**6. Testing and Maintenance**

* **Regular Testing:** Regular testing of the DRP to ensure its effectiveness and identify any gaps.
* **Maintenance:** Regular maintenance of backup systems, disaster recovery sites, and recovery procedures.

**7. Security and Compliance**

* **Security Measures:** Strong security measures to protect critical data and systems, including encryption, access controls, and security awareness training.
* **Compliance:** Adherence to industry standards and regulations, such as PCI DSS, HIPAA, and GDPR.

**8. Review and Updates**

This BCDR Policy will be reviewed and updated annually or as needed to reflect changes in the business environment and emerging threats.

By implementing a robust BCDR plan, the company can minimize the impact of disruptions, maintain business continuity, and protect its reputation

**Company Policy: Proper Internet Access for Ecommerce Site**

**Purpose**

This policy outlines guidelines for the appropriate and secure use of the company's ecommerce website. The goal is to protect customer data, maintain website integrity, and prevent unauthorized access.

**Acceptable Use**

1. **Authorized Access:** Only authorized employees with specific job responsibilities may access the ecommerce site's backend.
2. **Legitimate Business Purposes:** Access to the ecommerce site must be limited to legitimate business purposes, such as:
   * Processing orders
   * Managing inventory
   * Updating product information
   * Customer service inquiries
3. **Password Protection:** Employees must use strong, unique passwords to access the ecommerce site and change them regularly.
4. **Secure Login Procedures:** Employees must follow secure login procedures, including using multi-factor authentication if available.
5. **Data Privacy and Security:** Employees must handle customer data with the utmost care and adhere to data privacy regulations.
6. **Malware and Virus Protection:** Employees must keep their devices and browsers updated with the latest security patches to prevent malware infections.
7. **Phishing Awareness:** Employees must be aware of phishing attacks and avoid clicking on suspicious links or downloading attachments from unknown sources.

**Unacceptable Use**

1. **Unauthorized Access:** Accessing the ecommerce site without authorization is strictly prohibited.
2. **Misuse of Information:** Misusing customer data or using it for personal gain is strictly prohibited.
3. **Malicious Activities:** Engaging in malicious activities, such as hacking, data theft, or website vandalism, is strictly prohibited.
4. **Personal Use:** Using the ecommerce site for personal purposes, such as online shopping or social media, is not permitted during work hours.

**Monitoring and Enforcement**

1. **Access Logs:** The company may monitor access logs to identify unauthorized access or suspicious activity.
2. **Security Audits:** Regular security audits will be conducted to identify and address potential vulnerabilities.
3. **Violation of Policy:** Violations of this policy may result in disciplinary action, including termination of employment.

By adhering to this policy, employees can help protect the company's ecommerce site and ensure the security of customer data.

**Company Password Policy**

**Objective**

To enhance the security of company systems and data, this policy outlines the minimum password requirements for all employees.

**Password Requirements**

1. **Minimum Length:** All passwords must be at least 12 characters in length.
2. **Complexity:** Passwords must include:
   * At least two uppercase letters
   * At least two lowercase letters
   * At least two numeric digits
   * At least one special character (e.g., !@#$%^&\*()\_+-=[]{}|;':",.<>/?~)
3. **Dictionary Words:** Passwords must not contain any dictionary words, common phrases, or personal information.
4. **Password Expiration:** Passwords must be changed every 90 days.

**Password Best Practices**

* **Avoid Reusing Passwords:** Do not use the same password for multiple accounts.
* **Strong Password Creation:** Use a combination of upper and lowercase letters, numbers, and special characters.
* **Password Security:** Keep passwords confidential and avoid sharing them with others.
* **Password Storage:** Do not store passwords in plain text format.
* **Password Recovery:** Use strong password recovery questions and answers.

**Password Enforcement**

* **Password Reset:** Employees will be prompted to reset their passwords every 90 days.
* **Password Strength Checker:** A password strength checker will be implemented to help employees create strong passwords.
* **Password Policy Enforcement:** System administrators will enforce password policies through automated tools.

**Violation of Policy**

Failure to comply with this password policy may result in disciplinary action, including account.

**Company Policy: Customer Data Storage and Use**

**Purpose**

This policy outlines the guidelines for the collection, storage, use, and protection of customer data. The goal is to ensure data privacy, security, and compliance with applicable regulations.

**Scope**

This policy applies to all employees, contractors, and third-party service providers who have access to customer data.

**Data Collection and Storage**

1. **Data Minimization:** The company will only collect customer data that is necessary for the specific purpose for which it is collected.
2. **Data Accuracy:** The company will take reasonable steps to ensure that customer data is accurate and up-to-date.
3. **Data Security:** The company will implement appropriate technical and organizational measures to protect customer data from unauthorized access, disclosure, alteration, or destruction.
4. **Data Retention:** The company will retain customer data only for as long as necessary to fulfill the purpose for which it was collected or as required by law.

**Data Use**

1. **Permitted Uses:** Customer data may be used for the following purposes:
   * Providing products and services
   * Improving customer experience
   * Marketing and advertising
   * Research and development
   * Compliance with legal obligations
2. **Third-Party Sharing:** The company may share customer data with third-party service providers, but only if necessary to provide products or services and if appropriate safeguards are in place.
3. **Consent:** The company will obtain explicit consent from customers before sharing their data with third parties for marketing purposes.

**Data Privacy and Security**

1. **Data Breach Notification:** In the event of a data breach, the company will notify affected customers promptly and take appropriate steps to mitigate the impact of the breach
2. **Data Protection Officer:** The company will designate a Data Protection Officer (DPO) to oversee data privacy and security.
3. **Employee Training:** Employees will receive regular training on data privacy and security best practices.
4. **Regular Security Audits:** The company will conduct regular security audits to identify and address potential vulnerabilities.

**Compliance with Regulations**

The company will comply with all applicable data protection laws and regulations, including but not limited to:

* **GDPR (General Data Protection Regulation)**
* **CCPA (California Consumer Privacy Act)**
* **HIPAA (Health Insurance Portability and Accountability Act)**
* **PCI DSS (Payment Card Industry Data Security Standard)**\*

By adhering to this policy, the company aims to build trust with customers and protect their privacy.

**Company Policy: Acceptable Workplace Computer Usage**

**Purpose**

This policy outlines the guidelines for the appropriate and ethical use of company-owned computers, networks, and internet access. The goal is to ensure efficient productivity, maintain data security, and protect the company's reputation.

**Scope**

This policy applies to all employees, contractors, and authorized users of company-owned computers and networks.

**Acceptable Use**

* **Work-Related Activities:** Company computers and networks must be used primarily for work-related tasks, including:
  + Email communication
  + Accessing company databases and systems
  + Research and development
  + Customer service
  + Order processing
* **Limited Personal Use:** Limited personal use of company computers and networks may be permitted, provided it does not interfere with work responsibilities or violate company policy. Personal use may include:
  + Brief personal email checks

**Unacceptable Use**

* **Illegal Activities:** Engaging in any illegal activity, including hacking, unauthorized access, or copyright infringement, is strictly prohibited.
* **Harassment and Discrimination:** Using company computers for harassment, discrimination, or any form of offensive behavior is strictly prohibited.
* **Inappropriate Content:** Accessing or distributing inappropriate content, such as pornography or hate speech, is strictly prohibited.
* **Excessive Personal Use:** Excessive personal use that significantly impacts work productivity is not permitted.
* **Downloading and Uploading:** Downloading or uploading large files or unauthorized software without prior approval is prohibited.
* **Social Media:** Using social media for non-work-related purposes during work hours is generally discouraged.

**Data Security and Privacy**

* **Password Protection:** Employees must create strong, unique passwords and keep them confidential.
* **Data Confidentiality:** Employees must protect sensitive company data and customer information.
* **Secure Communication:** Employees must use secure communication channels to transmit confidential information.
* **Malware Protection:** Employees must be cautious about opening email attachments or clicking on suspicious links.
* **Reporting Security Incidents:** Employees must report any suspected security breaches or unauthorized access to IT immediately.

**Monitoring and Enforcement**

* **Monitoring:** The company reserves the right to monitor network traffic, email, and internet usage to ensure compliance with this policy and for security purposes.
* **Consequences of Violation:** Violations of this policy may result in disciplinary action, up to and including termination of employment.

**Review and Updates**

This policy will be reviewed periodically and updated as needed to reflect changes in technology or business practices.

By using company-owned computers and networks, employees agree to abide by this policy

**Email Policy**

**Objective**

To ensure the security and integrity of company email systems and data, this policy outlines guidelines for appropriate email usage.

**Email Usage**

1. **Work-Related Use:** Company email systems should be used primarily for work-related purposes, such as:
   * Communication with colleagues and clients
   * Sharing documents and files
   * Scheduling meetings
2. **Personal Use:** Limited personal use of company email may be permitted, provided it does not interfere with work responsibilities. However, excessive personal use is discouraged.
3. **Email Etiquette:** Employees should follow professional email etiquette, including:
   * Using clear and concise subject lines
   * Proofreading emails for errors
   * Responding to emails promptly
   * Avoiding the use of all-caps and excessive exclamation points

**Email Security**

1. **Password Protection:** Employees should create strong, unique passwords for their email accounts and avoid sharing them with others.
2. **Phishing Awareness:** Employees should be aware of phishing attacks and avoid clicking on suspicious links or opening attachments from unknown senders.
3. **Reporting Phishing Attempts:** Any suspected phishing emails should be reported to the IT department immediately.
4. **Secure Email Practices:** Employees should be cautious about sending sensitive information via email and consider using secure communication channels when necessary.
5. **Malware Prevention:** Employees should avoid opening attachments from unknown senders and scan attachments for viruses before opening them.

**Email Retention and Archiving**

1. **Email Retention:** The company will retain emails for a specified period, as required by legal and regulatory obligations.
2. **Email Archiving:** Emails may be archived for future reference and legal purposes.

**Violation of Policy**

Violation of this email policy may result in disciplinary action, including termination of employment.

By following this email policy, employees can help protect the company's email systems and data from security threats.

**Company Policy: Professional Workplace Phone Usage**

**Purpose**

This policy outlines guidelines for the appropriate and professional use of company-issued phones and personal phones for work-related purposes. The goal is to maintain a productive and respectful work environment while ensuring effective communication.

**Professional Phone Usage**

1. **Work-Related Calls:** Prioritize work-related calls and limit personal calls during work hours.
2. **Phone Etiquette:**
   * Answer calls promptly and professionally.
   * Speak clearly and concisely.
   * Use a courteous and respectful tone.
   * Avoid using speakerphone in public areas.
   * Minimize background noise during calls.
3. **Mobile Phone Usage:**
   * Use mobile phones for work-related purposes in a professional manner.
   * Avoid using mobile phones during meetings or important discussions.
   * Silence or vibrate mobile phones in meetings and quiet work areas.
4. **Conference Calls:**
   * Join conference calls on time and be prepared.
   * Mute your microphone when not speaking to avoid background noise.
   * Speak clearly and avoid interrupting others.

**Confidentiality and Security**

1. **Sensitive Information:** Avoid discussing sensitive or confidential information over unsecured phone lines.
2. **Data Privacy:** Protect personal and company data by using secure messaging apps and encryption when necessary.
3. **Password Protection:** Set strong, unique passwords for your company-issued phone and any related accounts.

**Violation of Policy**

Violation of this policy may result in disciplinary action, including verbal warnings, written warnings, or termination of employment.

By adhering to this policy, employees can contribute to a positive and productive work environment.