Policy of Prodapt IT

Third-Party Access Policy

Introduction
The Third-Party Access Policy defines how local or remote third parties can access Prodapt's corporate network, systems, and data. It applies to various third parties, including suppliers and contractors, and promotes the principle of least privilege for access.

Purpose
The policy aims to ensure that third-party organizations do not compromise the integrity, security, and privacy of Prodapt's customer data. It seeks to maintain confidentiality, integrity, availability, and accountability of information.

Scope
This policy covers all connections and access requests from third parties to Prodapt's network resources.

Policy Highlights

- **Access Management**: Access is granted based on defined operational roles, and requests must go through a Help Desk Ticket process.
- **Security Impact Analysis**: The IT team conducts analyses to ensure compliance with business requirements and the principle of least access.
- **Approval Process**: Access requires approvals from the Delivery Head and IT Head, and security audits must be performed for integrations.
- **Compliance Agreements**: Third parties must accept Prodapt' s Acceptable Use Policy and sign NDAs before accessing systems.
- **Periodic Reviews**: The IT team conducts quarterly reviews of third-party access to remove dormant or inactive accounts.
- **Access Revocation**: Access will be revoked when no longer needed or after a predefined period of inactivity.
- **Record Keeping**: Logs of all access modifications must be maintained.

Assuring Compliance
Before granting access, Prodapt ensures:

- Due diligence and compliance controls are in place.
- Written agreements define security requirements.
- Data in transit is encrypted, and access is limited to the minimum necessary duration.
- Standard agreements with customers and partners include security controls and responsibilities.

Third-Party Contracts
All contracts for third parties handling confidential data must include:

- Acknowledgment of security responsibilities.
- Requirements for regular reviews of security controls.
- Recourse for non-compliance and responsibilities for incident response.
- Specifications for data return or destruction upon contract termination.

Third-Party Review
For critical services or data, Prodapt must review the service provider's internal controls for compatibility with its security requirements, with annual reviews mandated post-establishment of the relationship.

Prodapt Email Policy Summary

Introduction

- The policy establishes guidelines for managing email as a critical resource.
- It aims to promote acceptable practices, educate users about their responsibilities, and set retention schedules.

Definitions

- **Email**: Any electronic communication sent or received within the email system.
- **Email Spoofing**: Forging an email header to mislead the recipient.
- **Anti-Spoofing**: A technique to identify and block spoofed emails.
- **Spam**: Unsolicited emails, often considered junk.

Purpose

- To ensure proper use of the email system and define acceptable and unacceptable usage.
- Applicable to all individuals with access to Prodapt's email resources.

Scope

- Covers all employees, vendors, and agents using Prodapt's email system.

Legal Obligations

- Individuals may be liable for sending offensive content, forwarding confidential information without permission, and distributing copyrighted material unlawfully.

Policy Guidelines

- **Privacy**: Corporate email is not private; Prodapt can monitor emails at any time.
- **Incoming Email**: Must be treated with care; antivirus applications are used for filtering.

- **Prohibited Actions**: Includes harassing emails, using email for personal business, sending spam, and violating copyright laws.
- **Confidential Information**: Sensitive information must be encrypted before being sent outside Prodapt's network.

Incidental Use

- Limited personal use is allowed but must not interfere with work duties or incur costs.

Email Retention and Archiving

- Emails are retained for 36 months, after which they may be automatically purged. Archived emails are also subject to this timeframe.

Discrimination and Harassment

- Emails containing discriminatory content are strictly prohibited, and violations can lead to disciplinary actions.

Ownership and Security

- Prodapt owns all email communications; management can access email content. Users must maintain strong passwords and avoid sharing their email accounts.

Phishing Awareness

- Users should be wary of unsolicited emails, avoid clicking on dubious links, and report suspicious emails immediately.

Email Disclaimer

- A confidentiality disclaimer is automatically appended to all outgoing emails (except internal communications).

Compliance

- Adherence to this policy is mandatory; violations may result in disciplinary action, including termination.

Exceptions

- Any exceptions to the policy must be approved by the Infosec team.

Prodapt Endpoint Security Policy Summary

Introduction

- The policy aims to protect the Prodapt network from security breaches caused by Endpoint devices (e.g., desktops, laptops, tablets, and mobile devices).
- It seeks to mitigate security threats by informing employees of requirements and restrictions regarding Endpoint devices and implementing security solutions.

Scope

- This policy applies to all Endpoint devices connected to the Prodapt network.

Policy Guidelines

- **Installation of Security Solutions**: The IT team is responsible for installing Endpoint Security Solutions, including Anti-Virus, Encryption, Data Loss Prevention, and Web Proxy, on all connected Endpoint devices to ensure compliance with Prodapt's policies.
- **Endpoint Software Requirements**: All Endpoint devices must have the required security software installed and running the latest versions/definitions prior to connecting to the Prodapt internal network.
- **Prohibition on Disabling Security Solutions**: Disabling or removing Endpoint Security Solutions or updates on any Endpoint device is strictly prohibited.
- **Firewall Requirements**: Endpoint devices capable of running local Firewall software must do so to protect against external threats.
- **Removable Media Restrictions**: The use of removable media storage devices (like USB drives or external hard disks) is restricted by default on all Endpoint devices.
- **Monitoring and Management**: The IT team will manage and monitor the connectivity and activity of Endpoint devices to detect and limit security threats.
- **Threat Isolation**: Any Endpoint device identified as posing a threat to the network's confidentiality, integrity, or availability may be disconnected, isolated, or restricted without prior notice.
- **Hardened Systems**: Desktop, laptop, and other IT infrastructure devices are to be hardened according to Prodapt Standards.
- **Blocking Malicious Sites**: Access to abuse, gaming, or phishing sites is blocked by default for all security groups.
- **Incident Management**: Security incidents will be managed according to the “Security Incident Management Process,” with disciplinary action for deliberate breaches or non-compliance.
- **Exceptions**: Any exceptions to the policy require approval from the IT Head along with proper business justification.

Prodapt Internet Usage Policy Summary

Introduction

- The policy establishes guidelines for managing Internet access as a valuable resource, aiming to create acceptable practices and educate users on their responsibilities.

Definitions

- **Internet**: A global network connecting various computers and networks.
- **Intranet**: A private network accessible only to authorized employees.

- **User**: An individual or application authorized to access Prodapt's resources.
- **World Wide Web (WWW)**: A system of Internet hosts that allows access to documents formatted in HTML.

Scope

- This policy applies to all individuals with access to Prodapt's information systems and Internet resources, ensuring guidelines are in place to protect employees from inappropriate material.

Policy Guidelines

- **Responsibility**: Employees must maintain the company's public image while using the Internet for ethical and lawful purposes.
- **Remote Access**: Internet access via Remote Desktop is permitted for business purposes only.
- **Blocked Categories**: Sites related to abuse, gambling, and games are blocked.
- **Secure Communication**: Internet communications should occur through approved channels, and no communications should be made under an assumed name.
- **Copyright Compliance**: Users cannot transmit copyrighted material without permission.
- **Prohibition of Personal Gain**: Internet use for personal gain or solicitation of non-company business is strictly prohibited.
- **Sensitive Information**: Personal Identifiable Information (PII) must not be sent over the Internet in plain text.

Accessing the Internet

- Users are granted Internet access for work-related tasks, which may be revoked at management's discretion. IT may restrict access to certain sites that threaten performance or security.
- All software must be part of the approved software suite and incorporate security patches.
- Direct access to the Internet bypassing Prodapt's network security is prohibited.

Expectation of Privacy

- Users have no expectation of privacy regarding anything created, sent, or received through Prodapt's Internet access.

File Downloads and Virus Protection

- Users cannot download or install software without authorization from IT. All downloaded files must be scanned for viruses.
- Deliberate propagation of malicious software is strictly prohibited.

Monitoring

- All Internet activity is subject to logging and review by Prodapt, including monitoring sites visited and communications.

Frivolous Use

- Users must conserve resources and avoid non-business-related Internet activities that monopolize network bandwidth.

Content Restrictions

- Access to inappropriate websites is blocked, and users must report accidental access to such sites.
- Hosting personal or non-Prodapt commercial sites without IT permission is prohibited.

Transmissions

- Sensitive material transmitted over the Internet must be encrypted, and electronic files must adhere to retention rules.

Incidental Use

- Limited personal use of the Internet is allowed but should not interfere with work duties or incur costs to Prodapt. All files are owned by Prodapt and may be accessed in accordance with this policy.

This summary captures the essential elements of the Internet Usage Policy at Prodapt. If you have any specific questions or require further details about any aspect, feel free to ask!

Prodapt Incident Management Policy Summary

Overview

- The Incident Management Policy provides a structured approach for responding to unplanned events (incidents) that could disrupt business operations.
- It aims to restore critical business functions quickly, identify weaknesses, mitigate impacts, and protect the organization's reputation and finances.

Purpose

- The policy guides employees on the appropriate response and timely reporting of computer security-related incidents (e.g., viruses, unauthorized activities) and non-IT incidents (e.g., power failures).
- It emphasizes the importance of developing and maintaining an incident management process.

Scope

- The policy applies to all Prodapt employees and contracted IT service providers when dealing with IT incidents.

- An incident is defined as any unauthorized action that compromises the confidentiality, integrity, or availability of information systems.

Roles and Responsibilities

- Implementation is managed by Prodapt IT personnel, who are responsible for identifying, responding to, and mitigating incidents.
- The Service Desk maintains an incident register, ensuring incidents are tracked and escalated appropriately.

Policy Guidelines

- Incidents must be detected and reported promptly by authorized personnel.
- Proper documentation and evidence collection are essential for investigations and to withstand scrutiny.
- Incidents should be dealt with swiftly to minimize operational disruptions and prevent recurrence.
- All employees must report incidents or near misses and are prohibited from attempting to prove suspected weaknesses.

Incident Management Process

- The policy outlines the procedures for identifying and prioritizing incidents, incident monitoring, detection, handling, and escalation.
- Severity levels classify incidents, and monitoring guidelines help track both physical and IT-related incidents.
- A comprehensive documentation process ensures all incidents are recorded, detailing the time discovered and actions taken.

Post-Incident Analysis

- After resolving an incident, a post-mortem analysis is conducted to evaluate procedures and identify improvements.
- The Infosec team leads this effort, ensuring lessons learned are integrated into future incident management efforts.

Emergency Planning

- Significant incidents affecting major services may be declared emergencies, prompting the formation of a Disaster Response Team to manage the situation according to established policies.

Compliance and Violations

- All Prodapt employees must adhere to the policy, and non-compliance may result in disciplinary action per HR policies.
- Any significant environmental changes must also be reported to IT promptly.

Documentation and Record Retention

- Incident logs and documentation must be maintained for at least one year or until an investigation is complete.
- Both digital and physical evidence must be preserved securely.

Prodapt Anti-Malware Policy Summary

Overview

- The policy addresses the need for protection of IT assets from malware and virus attacks, which can seriously disrupt operations and compromise sensitive information.

Purpose

- The primary aim is to promote the use of anti-virus and anti-malware software and educate employees on effective malware prevention practices, while also ensuring compliance with legal regulations.

Scope

- This policy applies to all Prodapt employees, contractors, and third-party employees who have access to Prodapt's IT assets, including all workstations and servers owned or leased by the company.

Responsibilities

- The Global Server Team or designated personnel are responsible for the implementation and enforcement of the anti-malware policy.

Policy Guidelines

- **Mandatory Software**: All workstations connected to the Prodapt network, as well as standalone systems, must utilize Prodapt-approved anti-virus and anti-malware software.
- **Software Integrity**: Employees must not disable or alter the settings of the anti-virus and anti-malware software in a way that reduces its effectiveness.
- **Automatic Updates**: The frequency of automatic updates for the anti-virus and anti-malware software should not be modified to decrease update frequency.
- **File Server Protection**: All file servers must also employ anti-virus and anti-malware software to detect and clean any malware that may affect shared files.
- **Incident Reporting**: Any malware that is not automatically cleaned by the software must be reported as a security incident to the Help Desk.
- **Preventive Controls**: Prodapt will implement controls to prevent and detect unauthorized mobile code and malicious code.
- **E-mail Protection**: All email gateways must use approved anti-virus software and comply with information security management system (ISMS) rules.

Compliance and Enforcement

- The Infosec team will verify compliance through methods such as audits and monitoring. Non-compliance may lead to disciplinary action, including termination of employment.

Record Keeping

- Records generated as part of the Anti-Malware Policy must be retained for two years, either in hard copy or electronic format, and will be audited annually.