XDR-TECHVAULT SOLUTIONS

INFORMATION SECURITY POLICY

Acceptable Use Policy (AUP)

Document Information:

- **Policy Owner:** Chief Information Security Officer (CISO)
- **Effective Date:** January 1, 2025
- **Last Reviewed:** December 16, 2024
- **Next Review:** December 16, 2025
- **Version:** 1.0
- **Classification:** Internal

TABLE OF CONTENTS

---

1. PURPOSE

This Acceptable Use Policy establishes guidelines for the appropriate use of XDR-TechVault Solutions' information technology resources, including but not limited to computer systems, networks, software applications, email, internet access, and mobile devices. This policy aims to protect company assets, ensure operational security, maintain compliance with legal and regulatory requirements, and establish clear expectations for all users regarding acceptable conduct when accessing company resources.

---

2. SCOPE

This policy applies to all individuals who access XDR-TechVault Solutions' IT resources, including:

- Full-time and part-time employees
- Contractors and consultants
- Temporary workers
- Third-party vendors with system access
- Interns and volunteers
- Any other individuals granted access to company technology resources

This policy covers all company-owned, leased, or managed IT resources, as well as personal devices used to access company data or systems (BYOD - Bring Your Own Device).

---

3. POLICY STATEMENTS

3.1 General Use and Ownership

3.1.1 All IT resources provided by XDR-TechVault Solutions remain company property and are intended primarily for business purposes.

3.1.2 Access to company IT resources is a privilege granted to facilitate job responsibilities and may be revoked at any time.

3.1.3 Users have no expectation of privacy when using company IT resources. The company reserves the right to monitor, access, and disclose information stored on or transmitted through company systems.

3.1.4 Users are responsible for all activities conducted through their assigned accounts and credentials.

3.2 Acceptable Use

Company IT resources may be used for:

3.2.1 Conducting legitimate business activities related to job responsibilities

3.2.2 Professional development and training approved by management

3.2.3 Limited reasonable personal use that does not interfere with business operations, violate any policy, or incur additional costs to the company (see Section 3.5 for details)

3.2.4 Communication with customers, partners, and vendors in a professional manner

3.2.5 Accessing company-approved cloud services and applications for business purposes

3.2.6 Collaboration with team members using approved communication platforms

3.3 Unacceptable Use

The following activities are strictly prohibited:

3.3.1 Accessing, storing, distributing, or transmitting illegal, offensive, discriminatory, or harassing content

3.3.2 Installing unauthorized software, applications, or browser extensions without IT approval

3.3.3 Attempting to bypass, disable, or circumvent security controls, firewalls, or authentication mechanisms

3.3.4 Sharing login credentials or allowing unauthorized individuals to use company accounts

3.3.5 Downloading, installing, or executing files from untrusted or suspicious sources

3.3.6 Using company resources for personal commercial gain or operating outside business activities

3.3.7 Accessing, modifying, or deleting data without proper authorization

3.3.8 Connecting unauthorized devices to the company network without IT approval

3.3.9 Using company resources to engage in cryptocurrency mining

3.3.10 Attempting to gain unauthorized access to systems, networks, or data (including penetration testing without approval)

3.3.11 Introducing malware, viruses, or other malicious code intentionally or through negligence

3.3.12 Excessive personal use that impacts work performance or consumes significant network resources

3.4 Internet and Email Use

3.4.1 Internet access is provided to support business activities. All internet usage is subject to monitoring and logging.

3.4.2 Users must exercise caution when clicking links or downloading attachments from emails, even from known senders.

3.4.3 Company email accounts are for business communication. All emails sent from company accounts represent XDR-TechVault Solutions.

3.4.4 Users must not send confidential or proprietary information via unencrypted email to external parties.

3.4.5 Chain letters, spam, and non-business-related mass mailings are prohibited.

3.4.6 Automatic email forwarding to external email addresses (personal Gmail, Yahoo, etc.) is prohibited without IT approval.

3.4.7 Users should be cautious of phishing attempts and report suspicious emails to the IT Security team immediately.

3.4.8 Streaming media (video/audio) for non-business purposes should be minimized to preserve bandwidth for business operations.

3.4.9 Visiting websites known to host malicious content, illegal material, or adult content is strictly prohibited.

3.5 Personal Use

3.5.1 Limited personal use of company IT resources is permitted provided it:

- Does not interfere with job performance or business operations
- Does not violate any other company policy
- Does not incur additional costs to the company
- Occurs primarily during break times or outside of regular work hours

3.5.2 Personal use is a privilege, not a right, and may be revoked if abused.

3.5.3 Examples of acceptable limited personal use include:

- Brief personal emails during lunch breaks
- Quick personal web browsing during breaks
- Emergency personal phone calls

3.5.4 Examples of unacceptable personal use include:

- Operating a personal business or side venture
- Excessive social media browsing during work hours
- Streaming entertainment content during business hours
- Large personal file storage or transfers
- Online gaming or gambling

3.5.5 Users remain subject to all security and acceptable use requirements during personal use.

3.6 Social Media and External Communications

3.6.1 Employees may access social media for business purposes when relevant to their job functions

(marketing, customer engagement, industry research, etc.).

3.6.2 When posting content that references XDR-TechVault Solutions, employees must:

- Clearly indicate they are expressing personal opinions, not official company positions (unless authorized to speak on behalf of the company)
- Not disclose confidential, proprietary, or non-public company information
- Maintain professionalism and avoid content that could damage the company's reputation

3.6.3 Only authorized personnel (Marketing, PR, Executive team) may post official company communications on social media platforms.

3.6.4 Employees must not use company logos, trademarks, or branding in personal social media without approval from Marketing.

3.6.5 Employees should be mindful that their online presence reflects on XDR-TechVault Solutions and avoid posting content that could be considered discriminatory, harassing, or offensive.

3.6.6 Customer information, project details, and internal company matters must not be discussed on social media without proper authorization.

3.6.7 Employees participating in industry forums, technical communities, or professional networks should exercise discretion when discussing company technologies or practices.

3.7 Security Responsibilities

All users must adhere to the following security practices:

3.7.1 Password Management:

- Create strong, unique passwords meeting company complexity requirements
- Never share passwords with anyone, including IT staff or managers
- Change passwords immediately if compromise is suspected

- Do not reuse passwords across multiple systems or accounts
- Use the company-approved password manager for storing credentials

3.7.2 Multi-Factor Authentication (MFA):

- Enable MFA on all systems that support it when accessing company resources
- Protect MFA devices and backup codes appropriately

3.7.3 Device Security:

- Lock workstations when leaving them unattended (use Windows+L or Mac equivalent)
- Keep operating systems and applications updated with latest security patches
- Enable full-disk encryption on laptops and mobile devices
- Report lost or stolen devices to IT Security immediately

3.7.4 Data Protection:

- Follow the Data Classification and Handling Policy for all company information
- Encrypt sensitive data when storing or transmitting outside company networks
- Do not store company data on personal cloud storage services (Dropbox, Google Drive personal, etc.) without approval
- Securely delete sensitive data when no longer needed

3.7.5 Physical Security:

- Do not leave devices unattended in public places
- Secure printed documents containing sensitive information
- Properly dispose of documents using shredders or secure disposal bins

3.7.6 Remote Work Security:

- Use company-provided VPN when accessing company resources from remote locations
- Ensure home networks are secured with strong passwords
- Do not allow family members or visitors to use company devices

3.7.7 Awareness and Vigilance:

- Complete all required security awareness training
- Stay informed about current security threats and company security communications
- Be suspicious of unusual requests, especially those involving credentials or financial transactions

3.8 Incident Reporting Requirements

3.8.1 Users must immediately report the following to the IT Security team (security@xdr-techvault.com):

- Suspected malware infections or system compromises
- Lost or stolen devices containing company data
- Suspected phishing emails or social engineering attempts
- Unauthorized access attempts or suspicious account activity
- Accidental disclosure of sensitive information
- Security vulnerabilities discovered in company systems
- Any violation of this policy by other users

3.8.2 Reports should be made as soon as possible, ideally within 1 hour of discovery for critical incidents.

3.8.3 Users will not face retaliation for good-faith reporting of security incidents, even if the incident resulted from their own error.

3.8.4 Failure to report known security incidents may result in disciplinary action.

3.8.5 The IT Security team will investigate all reported incidents and provide feedback to the reporter when appropriate.

---

4. ROLES AND RESPONSIBILITIES

4.1 Executive Management

- Endorse and support this policy
- Ensure adequate resources for policy implementation
- Lead by example in following policy requirements

4.2 Chief Information Security Officer (CISO)

- Overall accountability for policy implementation and enforcement
- Authorize exceptions to this policy
- Review and update policy annually

4.3 IT Security Team

- Monitor compliance with this policy
- Investigate policy violations and security incidents
- Provide security awareness training
- Implement technical controls to enforce policy requirements

4.4 Human Resources

- Include policy acknowledgment in onboarding process

- Address policy violations through disciplinary procedures
- Coordinate policy training requirements

4.5 Department Managers

- Ensure their teams understand and comply with this policy
- Report suspected violations to IT Security or HR
- Approve business justifications for exception requests

4.6 All Employees and Users

- Read, understand, and comply with this policy
- Complete required security awareness training
- Report security incidents and policy violations
- Protect company assets and information

---

5. COMPLIANCE AND ENFORCEMENT

5.1 Violations of this policy may result in disciplinary action up to and including termination of employment or contract, and may also result in civil or criminal penalties.

5.2 Disciplinary actions will be determined based on the severity and frequency of the violation, and may include:

- Verbal or written warning
- Suspension of system access privileges
- Mandatory additional training

- Termination of employment or contract
- Legal action if warranted

5.3 The company reserves the right to take immediate action to protect systems and data, including temporary suspension of access, pending investigation of policy violations.

5.4 Compliance with this policy is a condition of employment and system access.

---

6. EXCEPTIONS

6.1 Exceptions to this policy must be approved in writing by the CISO or designated security authority.

6.2 Exception requests must include:

- Business justification
- Risk assessment and mitigation plan
- Duration of exception (temporary exceptions preferred)
- Approval from department manager

6.3 Approved exceptions will be documented and reviewed periodically.

6.4 Emergency exceptions may be granted verbally but must be documented within 48 hours.

---

7. RELATED DOCUMENTS

This policy should be read in conjunction with:

- Information Security Policy (Master Policy)
- Data Classification and Handling Policy

- Access Control Policy
- Incident Response Policy
- Remote Work Security Policy
- BYOD (Bring Your Own Device) Policy
- Password Policy
- Employee Handbook

---

8. DEFINITIONS

IT Resources: All information technology assets including but not limited to computers, laptops, mobile devices, servers, networks, software applications, email systems, cloud services, and data storage systems.

Authorized User: Any individual who has been granted access to company IT resources through official company processes.

Confidential Information: Non-public company information including but not limited to customer data, financial records, proprietary technology, trade secrets, and employee personal information.

Malware: Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems, including viruses, ransomware, trojans, and spyware.

Social Engineering: Manipulation techniques used to trick individuals into divulging confidential information or performing actions that compromise security.

Phishing: Fraudulent attempts to obtain sensitive information by disguising communications as trustworthy entities.

VPN (Virtual Private Network): Encrypted network connection used to securely access company resources over the internet.

9. REVISION HISTORY

Version	Date	Author	Changes Made
1.0	December 16, 2024	CISO Office	Initial policy creation

10. POLICY APPROVAL

This policy has been reviewed and approved by:

Chief Information Security Officer
Signature: _____
Date: _____

Chief Executive Officer
Signature: _____
Date: _____

Chief Technology Officer
Signature: _____
Date: _____

Human Resources Director
Signature: _____
Date: _____

11. REFERENCES

This policy was developed with consideration of:

- NIST SP 800-53: Security and Privacy Controls
- ISO/IEC 27001: Information Security Management
- CIS Controls v8
- SOC 2 Trust Services Criteria

CONFIDENTIAL - INTERNAL USE ONLY