VELDTECH
IT & Network Solutions

Updated 7/1/2025

Information Security & Cybersecurity Framework

An IT Security Planning Document for Small Businesses

Table of Contents

(916) 345-3616

VELDTECH
IT & Network Solutions

Executive Overview

In today's hyper-connected environment, cyber threats are no longer speculative risks—they are persistent, evolving dangers that target organizations of every size and industry. Veldtech recognizes that protecting our clients, staff, systems, and sensitive data requires a disciplined, proactive approach to cybersecurity. This IT Security Plan establishes a comprehensive framework to mitigate the risks posed by malicious actors, operational disruptions, and accidental data loss.

Purpose and Objectives

This document defines the policies, controls, and practices that form the foundation of our cybersecurity program. Our objectives are to:

- Safeguard client and company information against unauthorized access, disclosure, or destruction.
- Ensure business continuity in the face of cyber incidents or system failures.
- Maintain compliance with relevant standards and contractual obligations.
- Foster a culture of security awareness and accountability across all levels of the organization.

The Threat Landscape

Cybercrime continues to grow in frequency and sophistication. Phishing attacks, ransomware, credential theft, and exploitation of unpatched systems represent critical threats to our operations and reputation. A single compromised account or device can lead to significant financial losses, regulatory penalties, and diminished client trust.

Our Approach

This framework applies a layered defense strategy encompassing:

- **Account Security**: Enforcing strong password policies and mandatory multi-factor authentication to reduce credential compromise.
- **Device Security**: Restricting administrative access, maintaining rigorous patching schedules, and deploying enterprise-grade antivirus and monitoring tools.
- **Data Security**: Centralizing file storage, applying least privilege principles, and requiring secure device enrollment before access is granted.
- **Backup and Recovery**: Implementing robust backup procedures and disaster recovery plans to protect data integrity and restore operations rapidly.
- **Incident Response**: Defining clear escalation paths, response workflows, and contact protocols to contain and remediate threats effectively.

Roles and Responsibilities

Cybersecurity is a ***shared*** responsibility. While Veldtech's Security Administrator oversees the implementation and enforcement of this plan, every staff member and contractor plays a vital role in protecting our systems. Adherence to these policies is mandatory and subject to periodic audit.

Commitment to Continuous Improvement

This IT Security Plan is a living document that will be reviewed regularly to incorporate emerging threats, technological advances, and changes to regulatory requirements. By maintaining a proactive security posture, Veldtech demonstrates its commitment to protecting our clients and our business.

(916) 345-3616

VELDTECH
IT & Network Solutions

Core Security Policies and Procedures

Emergency Contacts:
Veldtech's security officer is the designated point of contact for any and all security issues. The security officer is:

Stephen Veldhuizen
Security Administrator
Help Desk: (916) 345-3616
Emergency Cell Phone: (559) 737-8777

Incident Response Plan – Emergency Contacts:

Contact	Name	Phone	Email
Business Leader:			
Technical Contact:	Stephen Veldhuizen – Veldtech	(916) 345-3616	helpdesk@veldtech.com
Police:			
Legal:			
Bank:			
Insurance:			
Other:			
Other:			

Account Security

- **Passwords**: Passwords are required to have a minimum of 16 characters and include uppercase, lowercase, number, and special characters. All passwords must be generated by and stored in the company Password Manager. Passwords must be completely random and may not contain any known words, phrases, names, numbers, or common patterns. Exceptions are made for passwords that must be entered by hand, where passphrases are acceptable. Passphrases must be a minimum of four uncommon words interspersed with randomly capitalized letters, numbers, and special characters.
- **Multi-Factor Authentication**: All accounts and logins are protected with Multi-Factor Authentication (MFA). Acceptable forms of MFA include:
    - Duo Mobile
    - TOTP
    - Fido security keys

  SMS and Email are unacceptable forms of MFA.
- **User Accounts**: Email and Password Manager accounts use Microsoft Entra SSO or are protected by Duo Mobile MFA. Staff are prohibited from using any free, personal, or consumer accounts (i.e. Gmail, Yahoo, Outlook, etc.) on their machines. All other logins are centrally managed by IT and use the staff business email address as the username or another centrally managed naming scheme.

[Continued on Next Page]

- **Account Sharing**: Users are prohibited from sharing accounts with other users unless said account is identified by management as a shared access account. User computer logins/email accounts may never be shared by multiple users. Users may not give the password to their account to any other user unless approved in writing by their manager and the IT department.

Device Security

- **Workstations**: Only IT is permitted Administrator access. Users are permitted to login to workstations with their unique user ID only, not a shared user account or local account.
- **Kiosks**: Devices meant for public use or customer access are defined as Kiosks. All kiosks are clearly defined and identifiable as a kiosk. Kiosks are isolated from the staff network and may only access data deemed client accessible.
- **Servers**: All on-premise servers are managed and maintained by IT. Only IT is permitted Administrator access. Physical server access should be limited to authorized individuals.
- **Mobile Devices**: All mobile devices with access to business resources (i.e. Email, files, phone calls, etc.) are enrolled in the company MDM. Personal mobile bring-your-own-devices (i.e. devices not owned by the company) are only allowed access to business resources after they are enrolled in the company MDM. All other mobile devices are prohibited from accessing business resources.
- **Updates**: All workstations and servers are configured to automatically download and install updates. If an update requires a restart, the user is notified. Updates are installed automatically once a week on a set schedule. If the device is off or offline, updates install the next time it powers on or connects to the internet.
- **Other Software**: All other software is configured to update automatically.
- **Anti-Virus**: Company managed anti-virus and security software is installed on all workstations used for business operations. Anti-virus is configured to automatically update and protect workstations.
- **Bring Your Own Device (BYOD):** Personal devices are prohibited from accessing company resources unless enrolled in company-managed device management and security software. BYOD devices must adhere to the same security and configuration standards as company-issued devices. Such devices may not be shared with family members or any other individuals. Any BYOD devices approved for use will be locked down to company standards and are subject to monitoring and audit by IT.

Data Security

- **File Storage**: All sensitive company files are stored in a centrally managed file storage solution (i.e. File Server or SharePoint).

[Continued on Next Page]

- **User Data**: Users are prompted to redirect known folders (i.e. Desktop, Documents, Pictures) to OneDrive. Users may only save files to approved storage locations, which are:
    - File server
    - SharePoint
    - OneDrive redirected folders

  Users are prohibited from saving files directly to their workstation in locations not redirected to OneDrive or the company file server.
- **Least Privileged Access**: Staff access to company data is limited to only the data needed to carry out their roles and responsibilities.
- **Data Access**: Only pre-approved devices enrolled in the company device management and security software are authorized to access company data.

Backup and Disaster Recovery

- **Device Backups**: Servers automatically backup daily at 12am. Workstations tagged for backup automatically backup daily at 12am. Backups are centrally stored by IT. 7 daily backups, 1 monthly backup, and 1 yearly backup are maintained.
- **Cloud Service Backups**: Email and cloud file servers are backed up via a SaaS backup service. The SaaS backup service is configured to automatically backup:
    - Email 1x day
    - Contacts 1x day
    - Calendars 1x day
    - Tasks 1x day
    - SharePoint/OneDrive 3x day
    - Groups/Teams 3x day
    - Private Chat 1x day
- **Encryption**: Backups are encrypted to protect data from unauthorized access. Encryption in transit and at rest is enforced across all sensitive data.
- **Backup and Disaster Recovery Testing**: To ensure the availability and integrity of backup data, backup restoration tests are performed at least annually. Tests involve restoring critical systems and data to confirm backups work correctly. Results of restoration tests are documented and reviewed by IT leadership. Any issues identified during testing are addressed promptly to maintain readiness.

Risk Management

- **Security Awareness Training**: All staff and contractors are required to complete annual Security Awareness Training to reinforce their understanding of cybersecurity threats and responsibilities. Training will cover:
    - Identification and reporting of phishing and social engineering attempts.
    - proper data handling practices.
    - secure use of company resources.

  Additional role-based training is provided to employees with elevated privileges or access to sensitive data. Periodic phishing simulations will be conducted to measure awareness and improve response readiness.

[Continued on Next Page]

- **Vulnerability Management**: All company systems are subject to regular vulnerability scanning to identify missing security updates and potential exposures. Vulnerability scans are performed at least quarterly and after significant changes to the environment. Identified vulnerabilities are prioritized based on severity and risk to the organization. Critical and high-severity vulnerabilities must be remediated as soon as reasonably possible. Vulnerability management activities are documented and reviewed by IT leadership.
- **Logging and Monitoring**: Critical systems, including servers, firewalls, and security appliances, are configured to generate audit logs of security-relevant events such as authentication attempts, administrative actions, and system changes. Audit logs are kept for at least one year and reviewed regularly to detect suspicious or unauthorized activity. When possible, logs are stored in a central system to protect their integrity and support monitoring. Access to audit logs is restricted to authorized IT personnel.
- **Secure Disposal**: All media containing sensitive or confidential information must be securely disposed of when no longer required. Hard drives, removable media, and other storage devices are securely erased or physically destroyed before disposal. Documentation of secure disposal is maintained for audit purposes. End users are prohibited from discarding any storage media without approval from IT.
- **Third-Party Risk Management**: Veldtech requires that all vendors and service providers with access to company systems or data meet appropriate security requirements. Before engaging any third party, IT management performs a risk assessment and reviews contracts to confirm security requirements. Where applicable, third parties must provide evidence of security controls, such as compliance certifications or audit reports. Vendor security performance is reviewed periodically.

Alignment with Industry Standards and Guidelines

Compliance Alignment
Veldtech is committed to maintaining a security posture that not only protects our systems and client data but also aligns with established industry standards and regulatory expectations. While this IT Security Plan is designed to serve as a comprehensive internal framework, it is informed by and supports compliance with the following standards and guidelines:

NIST Cybersecurity Framework (NIST CSF)
Veldtech's policies and procedures incorporate the core functions of the NIST Cybersecurity Framework—Identify, Protect, Detect, Respond, and Recover—to provide a structured approach to cybersecurity risk management. Our emphasis on asset identification, layered security controls, continuous monitoring, and defined incident response protocols demonstrates alignment with NIST CSF principles.

ISO/IEC 27001
The policies outlined in this plan reflect the risk-based approach, governance structure, and continuous improvement practices described in ISO/IEC 27001. Veldtech supports the development and maintenance of an information security management system (ISMS) that prioritizes the confidentiality, integrity, and availability of critical information assets.

CIS Critical Security Controls
This plan draws on the Center for Internet Security (CIS) Critical Security Controls to prioritize safeguards proven to reduce the likelihood and impact of cyber incidents. Specific measures, such as strict account management, endpoint protection, network segmentation, and regular vulnerability remediation, align with these prioritized controls.

HIPAA Security Rule
For clients subject to the Health Insurance Portability and Accountability Act (HIPAA), this framework includes administrative, physical, and technical safeguards necessary to protect electronic protected health information (ePHI). These controls support compliance with the HIPAA Security Rule's requirements for access controls, audit logging, integrity protections, and secure data transmission.

PCI DSS
For engagements involving payment card data, Veldtech's security practices are designed to assist clients in meeting the Payment Card Industry Data Security Standard (PCI DSS). This includes secure authentication practices, strict access controls, encryption of cardholder data, vulnerability management, and continuous monitoring of cardholder environments.

Continuous Improvement
This IT Security Plan will be reviewed regularly and updated to reflect changes in regulatory requirements, emerging threats, and evolving best practices. Veldtech remains committed to protecting client and business information by adhering to proven standards and demonstrating accountability at every level of the organization.

Cybersecurity Risk Assessment Worksheet

VELDTECH
IT & Network Solutions

Instructions

Use the following tables to identify sensitive company assets and data that should be protected by the security policies and procedures outlined in this document.

Identify Cybersecurity Risk to Your Business – Assets

Software, Hardware, System, Service:	Asset's Official Use:	Who Is the Asset Owner or Administrator?	Sensitive Data ON or ACCESSED by Asset:	Is MFA Required to Access Asset?	Risk to Business If We Lose Access to This Asset?

Identify Cybersecurity Risk to Your Business – Multi-Factor Authentication

Account:	MFA Enabled (Y/N):
Banking Account(s)	
Accounting and Tax Account(s)	
Merchant Account(s)	
Google, Microsoft, and Apple Account(s)	
Email Account(s)	
Password Manager(s)	
Website Account(s)	
CRM, ERP Account(s)	
VPN	

[Continued on Next Page]

VELDTECH
IT & Network Solutions

Identify Cybersecurity Risk to Your Business – Network Security

Hardware	Security Policy	Is the Security Policy Implemented (Y/N)?
Perimeter and Core Network Security (most critical, foundational controls):		
Router/Firewall	Remote access is limited by geolocation and/or by whitelist.	
Router/Firewall	Traffic filtering is configured to block malicious traffic.	
VPN	Accounts require both credentials and a user certificate.	
Internal Network Infrastructure:		
Switches	Management interfaces restricted to VLANs; SNMP secured with strong credentials.	
Wireless Access Points	Wireless networks require WPA3 encryption; guest networks are isolated in a separate VLAN.	
Server and Endpoint Systems:		
Servers	Web accessible servers are isolated in a separate VLAN.	
Workstations	User accounts do not have local administrator privileges; only IT staff are granted administrative access to devices.	
Supporting / Peripheral Devices:		
Printers	Default passwords are changed and firmware updated.	
Backup Appliances	MFA enforced; backups encrypted; devices isolated.	
VoIP Phones	Voice VLANs configured; firmware updated; admin access restricted.	

(916) 345-3616