

# HALTEC CORPORATION

SUPPLIER AND THIRD-PARTY SECURITY POLICY

***3/24/2025 – Version 2***

## 1. Executive Summary

This policy establishes security requirements for suppliers, vendors, and third-party partners who access, process, store, or transmit Haltec Corporation's information or provide services that impact the security of Haltec's systems

## 2. Scope

This policy applies to all third-party entities, including suppliers, vendors, contractors, and service providers, that interact with Haltec's information assets, systems, or infrastructure.

## 3. Security Requirements

### 3.1 Access Control

- Third parties must have explicit approval to access Haltec's information systems.
- Multi-factor authentication (MFA) must be used for remote and privileged access.
- Access must be granted based on the principle of least privilege and revoked upon contract termination or role change.
  - Any external software must be approved by Jeff Kovacich (VP of IT)

### 3.2 Data Protection and Confidentiality

- Confidential and sensitive data must be handled in accordance with compliance standards and classification requirements.
- Encryption must be used for transmitting and storing sensitive data.
- Third parties must not share, sell, or disclose Haltec's data without prior authorization.

### 3.3 Security Assessments and Compliance

- Third parties may be requested to undergo security assessments before engagement and periodically thereafter.
- Evidence of compliance with industry standards (e.g., ISO 27001, TISAX, SOC 2) may be required.
- Haltec reserves the right to audit third-party security controls to ensure compliance.
  - Vender assessments can be conducted on any critical IT services by VP of IT - Jeff Kovacich

### 3.4 Incident Response and Reporting

- Third parties must report security incidents affecting Haltec's data or systems within 24

hours.

- A documented incident response plan must be in place to address breaches, data leaks, and cyber threats.
- Cooperation with Haltec's IT Security Team is required for investigation and remediation efforts.

### 3.4.5 Risk assessments -

- carried out both at regular intervals and in response to events.
- Information security risks are assessed to utmost degree
- All Information security risks are documented in SharePoint
- The responsible risk owner (Jeff Kovacich) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.

### 3.5 Network and System Security

- Third parties must implement security controls such as firewalls, intrusion detection, and endpoint protection.
- Regular security patching and updates must be applied to prevent vulnerabilities.
- Unauthorized software or devices must not be connected to Haltec's network.

### 3.6 Secure Development and Maintenance

- Software and systems provided to Haltec must follow secure coding practices.
- Third parties must remediate security vulnerabilities promptly upon discovery.
- Access to Haltec's development or production environments requires prior approval.

## 4. Compliance and Legal Obligations

- Third parties must comply with all applicable laws, regulations, and contractual obligations regarding data protection and cybersecurity.
- Non-compliance may result in termination of contracts, legal action, or financial penalties.

## 5. Monitoring and Enforcement

- Haltec reserves the right to monitor third-party compliance with this policy.
- Violations may result in contractual penalties, service suspension, or legal action.
- Continuous security improvement and training must be demonstrated by third parties.

Version 2 Changes:

- Added a Risk Assessments section (3.4.5)
- Added the following to Security Requirements (3) *“Any external software must be approved by Jeff Kovacich (VP of IT)” & “Vender assessments can be conducted on any critical IT services by VP of IT - Jeff Kovacich”*