VIRASHIELD

TECHNOLOGIES INC.

ENTERPRISE INFORMATION SECURITY POLICY FRAMEWORK

Course Project: Developing Information Security Policies

B 1925 UNIVERSITY OF BALTIMORE

PREPARED FOR

625: Information System, Threats, Attacks, and Defense Strategies

Prepared by

Jeel Piyushkumar Khatiwala

Table of Content

1 Company Background Information

1.1 Company Name

ViraShield Technologies Inc.

1.2 Industry

Cybersecurity & Consumer Electronics

1.3 Company Size

500 employees

1.4 Headquarters & Global Presence

ViraShield is headquartered in Austin, Texas, USA. The company maintains international engineering and logistics centers in:

- Frankfurt, Germany (EU compliance and distribution)
- Bangalore, India (R&D and support)
- Singapore (APAC operations)

ViraShield currently supports customers in over 30 countries, including the United States, Germany, India, Singapore, Brazil, and South Africa, with compliance operations tailored to meet regional regulatory requirements in the U.S., EU, APAC, and LATAM markets.

1.5 Company Mission

To empower everyday users with enterprise-grade real-time antivirus protection through portable, plug-and-play devices that work seamlessly across platforms — laptops, TVs, smartphones, tablets, and IoT systems.

1.6 Core Product

The flagship product, **ViraShield Portable AV**, is a USB-based plug-and-play antivirus device designed for cross-platform real-time threat protection. Built with both USB-A and USB-C interfaces, the device supports laptops, desktops, smart TVs, mobile phones, tablets, and even vehicle infotainment systems.

Once connected to a compatible host device, the antivirus engine activates autonomously without requiring installation, user registration, or login credentials. The product offers:

- **Plug-and-Protect Functionality**: The device immediately begins scanning the host system for malware using embedded threat intelligence.
- **On-Device AI Engine**: Powered by a machine learning model trained on behavioral patterns of known malware, the device detects anomalies even in offline environments.

- **Subscription-Based Licensing**: The device communicates securely with ViraShield's cloud to validate the license key. Devices without an active subscription default to limited scan mode and display a renewal message via the host screen.
- **OTA (Over-the-Air) Updates**: Using TLS 1.3 encrypted channels, the device downloads the latest malware signatures and firmware updates periodically when internet access is available.
- **Cloud-Assisted Threat Telemetry**: With user consent, anonymized threat logs can be uploaded for research and global pattern recognition, enabling faster signature evolution.
- **Offline Functionality**: Users without internet can continue to scan using cached signatures. However, a defined **Offline Signature Expiry Policy** restricts full functionality after a pre-set time limit (e.g., 14–30 days).
- **Tamper-Resistant Design**: The device is physically hardened with epoxy-sealed chips, secure boot processes, and anti-reverse engineering measures.

ViraShield Portable AV is not a SaaS product but rather a hardware security appliance with cloud-assisted capabilities, designed to provide on-demand, portable protection without dependency on full-time connectivity or complex installations. is a USB-based dual-interface (Type-A/C) device that initiates real-time antivirus scanning the moment it is plugged into a host system. It functions without installation or login, drawing real-time threat signatures via secure OTA updates linked to an active subscription.

1.7 Key Technologies Used

- Embedded ARM Cortex-based microcontroller with secure enclave
- AI-powered threat detection engine (signature + behavioral models)
- On-device encrypted temporary log storage
- TLS 1.3-secured connection to AWS and Azure cloud endpoints
- OTA firmware and malware signature update framework
- Dynamic license validation and renewal service
- Microsoft 365 & Exchange (corporate communication, document collaboration)
- Jira, GitHub Enterprise, Jenkins (CI/CD & source control for development)
- AWS & Azure (cloud-based backend infrastructure, licensing system, threat telemetry ingestion)
- Salesforce / HubSpot CRM (customer support & subscription management)
- CrowdStrike or SentinelOne (internal EDR solutions)

- SIEM tools like Splunk or Wazuh (monitoring and log correlation)
- Mobile Device Management (for global endpoint policy enforcement)

1.8 Data Types Handled

- **PII**: Customer names, emails, shipping details (opt-in accounts only)
- **PCI**: Encrypted credit card data handled via Stripe and PayPal (never stored locally)
- **PHI**: When used by healthcare clients for scanning EHR-connected devices
- **Device Metadata**: OS type, manufacturer ID, usage timestamps
- **Threat Intelligence**: Detected malware behaviors and signatures
- **IP**: Proprietary firmware, AI models, and activation algorithms
- **Employee PII**: HR files, payroll data
- **Business Contracts**: Vendor agreements, NDAs
- **Operational Logs**: Development pipeline logs, system events
- **Financial Records**: Internal accounting systems
- **Client Data**: If support team collects data during RMA or issue diagnosis
- **Audit Logs**: Security logs from cloud or endpoint infrastructure

1.9 Threat Landscape

Due to the nature of its hardware product and cloud integration, ViraShield faces a complex threat environment:

- **Firmware reverse engineering** to clone or bypass device functions
- **USB spoofing or counterfeiting** to mimic official ViraShield hardware
- **Phishing and social engineering** against support agents
- **Cloud API abuse** or DDoS against license verification systems
- **Supply chain tampering** during manufacturing or shipping
- **Insider threats** targeting R&D or licensing secrets
- **Zero-day malware** undetected by outdated devices
- **Credential stuffing & phishing attacks** on internal teams (esp. support/sales)
- **SaaS misconfigurations** in Jira, M365, or GitHub
- **Data leakage from misconfigured buckets (S3, Azure Blob)**
- **Rogue access or unapproved** shadow IT by remote teams
- **Insider data exfiltration** using developer tools or USB devices
- **Legal and compliance risks** related to GDPR and HIPAA audits

1.10 Regulatory & Security Compliance Requirements

ViraShield operates under a broad set of international and industry-specific compliance regimes that support its product operations, licensing architecture, and internal IT infrastructure:

- **GDPR** – For customer privacy, telemetry consent, and data subject rights in the EU
- **CCPA** – Consumer data disclosures and opt-out rights in California
- **HIPAA** – For scanning EHR-integrated devices in clinical settings
- **PCI DSS** – Secure online payment processing (Stripe, PayPal)
- **ISO/IEC 27001** – Certified ISMS controls across company and product operations
- **ISO/IEC 27701** – Privacy Information Management aligned with GDPR and cross-border data flows
- **ISO/IEC 27017** – Cloud service security controls for AWS/Azure backend
- **NIST SP 800-53** – Access controls, system integrity, account management
- **NIST SP 800-61** – Incident response lifecycle for breach handling
- **NIST SP 800-171** – Protection of controlled unclassified information (CUI)
- **NIST SP 800-40** – OTA patching and update protocols
- **NIST SP 800-161** – Supply chain security for hardware manufacturing and delivery
- **MITRE ATT&CK** – Threat detection modeling in ViraShield's cross-platform analytics engine

1.10.1 Compliance-Supported Countries by Region

Region	**Countries**	**Relevant Frameworks Support**
North America	United States, Canada, Mexico	CCPA, HIPAA, NIST SP 800-53/61/171, PCI DSS, ISO/IEC 27001, ISO/IEC 27017
Europe (EU/EEA)	Germany, France, United Kingdom, Netherlands, Spain, Italy, Sweden, Finland, Poland, Ireland	GDPR, ISO/IEC 27701, ISO/IEC 27001, NIS2 Directive (EU), ENISA Recommendations
Asia-Pacific	India, Singapore, Japan, South Korea, Australia, New Zealand, Malaysia, Indonesia, Philippines	India DPDP 2023, Singapore PDPA, Japan APPI, South Korea PIPA, ISO/IEC 27001, Regional Localization Laws, APAC-specific breach and consent requirements

Middle East & Africa	United Arab Emirates, Saudi Arabia, Egypt, South Africa	Local Cybersecurity Frameworks, ISO/IEC 27001, GDPR-inspired regional laws, Global Regulatory Compliance Policy (internal mapping to maintain alignment)
South America	Brazil, Argentina, Chile, Colombia, Nigeria (included for Pan-African alignment)	Brazil LGPD, ISO/IEC 27001, Global Regulatory Compliance Policy, country-specific e-privacy and retention rules

Note: This table lists the 30 countries where ViraShield products are supported, along with the compliance frameworks that align with each region's regulations.

1.10.2 Enterprise Policy Inventory Overview

This table outlines all finalized security and compliance policies implemented by ViraShield Technologies Inc., categorized by functional domains. Each policy is aligned with relevant frameworks, includes an assigned policy number, and reflects official responsibility and review cadence.

ViraShield Technologies Inc. - Master Security Policy Inventory

Policy Inventory Summary This table outlines all finalized security and compliance policies implemented by ViraShield Technologies Inc., categorized by functional domains. Each policy is aligned with relevant frameworks, includes an assigned policy number, and reflects official responsibility and review cadence.

No.	Policy Name	Category	Framework(s) Referenced	Policy Owner
1	Identity and Access Management (IAM) Policy	Employee & Internal Access Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.5)	Chief Information Security Officer (CISO)
2	Acceptable Use Policy	Employee & Internal Access Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.5)	HR Director / IT Security
3	Remote Work Security Policy	Employee & Internal Access Policies	NIST SP 800-46, ISO/IEC 27001:2022 (Annex A.6)	Director of IT

4	Employee Onboarding & Offboarding Policy	Employee & Internal Access Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.7)	HR Manager
5	Insider Threat Detection Policy	Employee & Internal Access Policies	NIST SP 800-53, CERT Guide	Insider Threat Program Manager
6	Firmware Integrity and Code Signing Policy	Firmware & Product Development Policies	NIST SP 800-147, ISO/IEC 27001:2022 (Annex A.8)	Director of Firmware Security
7	Secure Code Development Policy	Firmware & Product Development Policies	NIST SP 800-53, NIST SSDF, OWASP SAMM	Lead Software Security Architect
8	Intellectual Property Protection Policy	Firmware & Product Development Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.8)	Director of Legal / R&D Security
9	Device Hardening Policy	Firmware & Product Development Policies	NIST SP 800-53, NIST IoT Guidelines	Device Engineering Manager
10	Third-party Component Validation Policy	Firmware & Product Development Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.15)	Director of Supply Chain Security
11	Privacy and Telemetry Consent Policy	Customer Data & Privacy Policies	NIST SP 800-53, GDPR, ISO/IEC 27701	Chief Privacy Officer
12	Customerless Device Use Policy	Customer Data & Privacy Policies	NIST SP 800-53, GDPR Recital 26, ISO/IEC 27701	VP of Product Compliance
13	Customer Data Handling & Retention Policy	Customer Data & Privacy Policies	NIST SP 800-53, GDPR, ISO/IEC 27001:2022 (Annex A.8)	Chief Data Protection Officer

14	GDPR & CCPA Compliance Policy	Customer Data & Privacy Policies	NIST SP 800-53, GDPR, CCPA, ISO/IEC 27701	Regional Compliance Officers (US/EU)
15	Product Activation & Subscription Policy	Licensing & Subscription Policies	Internal Logic, PCI DSS	Director of Subscription Services
16	Payment Processing Policy	Licensing & Subscription Policies	PCI DSS	VP of Finance
17	License Key Verification & Renewal Policy	Licensing & Subscription Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.9)	Director of Licensing Operations
18	Account Termination and Data Deletion Policy	Licensing & Subscription Policies	NIST SP 800-53, GDPR, CCPA	Chief Privacy Officer
19	Cloud Security Policy	Cloud Infrastructure Policies	NIST SP 800-53, ISO/IEC 27017	Cloud Infrastructure Manager
20	Encryption and Key Management Policy	Cloud Infrastructure Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.10)	Cryptographic Security Lead
21	Logging and Monitoring Policy	Cloud Infrastructure Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.12)	SOC Manager
22	Network Segmentation & Firewall Policy	Cloud Infrastructure Policies	NIST SP 800-53, CIS Controls	Network Security Architect
23	Incident Response Policy	Incident Response & Continuity Policies	NIST SP 800-61, ISO/IEC 27001:2022 (Annex A.16)	Incident Response Manager
24	Backup & Disaster Recovery Policy	Incident Response & Continuity Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.17)	Director of IT Operations

25	Breach Notification Policy	Incident Response & Continuity Policies	NIST SP 800-53, GDPR, HIPAA	Chief Privacy Officer
26	Business Continuity Plan (BCP)	Incident Response & Continuity Policies	NIST SP 800-53, ISO 22301	VP of Risk and Resilience
27	Cross-Platform Threat Analytics Policy	Specialized Product Security Policies	NIST SP 800-53, MITRE ATT&CK	Director of Threat Intelligence
28	Device Spoofing and Counterfeit Prevention Policy	Specialized Product Security Policies	NIST SP 800-53, NIST SP 800-207	Hardware Security Engineering Lead
29	Offline Signature Expiry Policy	Specialized Product Security Policies	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.14)	Detection Engine QA Lead
30	Subscription Lock & Deactivation Policy	Specialized Product Security Policies	NIST SP 800-53, Internal Logic	Licensing Security Lead
31	Global Regulatory Compliance Policy	Regional & Global Compliance Policies	NIST SP 800-53, GDPR, India DPDP, Singapore PDPA	Chief Compliance Officer
32	Hardware Lifecycle Security Policy	Hardware Lifecycle Policies	NIST SP 800-53, NIST SP 800-88, ISO/IEC 27001:2022 (Annex A.11)	Director of Hardware Operations
33	Supply Chain Security Policy	Hardware Lifecycle Policies	NIST SP 800-161, ISO/IEC 27001:2022 (Annex A.15)	Supply Chain Security Manager
34	Antivirus Detection Engine Development Policy	Threat Intelligence, AI & Engine Policies	NIST SP 800-83, ISO/IEC 27034	Director of AV Engineering
35	Antivirus Scanning Behavior Policy	Threat Intelligence, AI & Engine Policies	AMTSO Standards, Internal Logic	AV Engine Design Team Lead
36	AI/ML Model Security Policy	Threat Intelligence, AI & Engine Policies	NIST SP 800-53, ISO/IEC 27034	AI Security Officer

37	Threat Intelligence Sharing & Signature Update Policy	Threat Intelligence, AI & Engine Policies	NIST SP 800-150, ISO/IEC 27001:2022 (Annex A.13)	Threat Intel and Detection Sharing Manager
38	Firmware Update Rollback Protection Policy	OTA & System Resilience Policies	NIST SP 800-193	Firmware Security Lead
39	Secure OTA Update Validation Policy	OTA & System Resilience Policies	ISO/IEC 27001:2022 (Annex A.14)	OTA Pipeline Lead
40	Signature Downgrade Detection & Expiry Alert	OTA & System Resilience Policies	Internal Logic	Device Firmware Team
41	Embedded Device Internet Communication Policy	OTA & System Resilience Policies	NIST SP 800-213	Embedded Networking Engineer
42	Physical Tamper Response Policy	Internal Monitoring & Regional Data Protection	NIST SP 800-161	Director of Facility Security
43	Vulnerability Management Policy	Internal Monitoring & Regional Data Protection	NIST SP 800-40, ISO/IEC 27001:2022 (Annex A.12)	Vulnerability Management Lead
44	Insider Threat Prevention & Monitoring Policy	Internal Monitoring & Regional Data Protection	NIST SP 800-53, ISO/IEC 27001:2022 (Annex A.7)	Insider Threat Program Coordinator
45	Product-Specific Malware Incident Policy	Internal Monitoring & Regional Data Protection	NIST SP 800-61	Director of Product Security
46	Portable Device Compatibility Assurance Policy	Internal Monitoring & Regional Data Protection	Internal QA Standards	Director of Quality Assurance

47	Regional Data Protection Policy (APAC)	Internal Monitoring & Regional Data Protection	Singapore PDPA, India DPDP	Chief Privacy Officer

2 Employee & Internal Access Policies

2.1 Identity and Access Management (IAM) Policy

Frameworks: NIST SP 800-53 (AC-1 to AC-17), ISO/IEC 27001:2022 (Annex A.5)

Policy #: VS-IAM-001

Policy Title: Identity and Access Management (IAM) Policy

Policy Owner: Chief Information Security Officer (CISO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Mandatory

2.1.1 Purpose

This policy defines the required controls and procedures for managing user identity lifecycle and system access privileges across all ViraShield Technologies Inc. environments. It ensures secure authentication, role-based authorization, session monitoring, and timely deprovisioning in accordance with applicable compliance standards.

2.1.2 Scope

This policy applies to:

- All employees, contractors, interns, and vendors accessing company systems
- All internal systems including cloud (AWS, Azure), on-prem infrastructure, internal development platforms (Jira, GitHub, Jenkins), CRM (HubSpot), and MDM platforms
- All customer-facing cloud endpoints that perform licensing, telemetry, or OTA operations
- ViraShield hardware platforms and associated manufacturing/QA tools

2.1.3 Policy Statement

2.1.3.1 Identity Lifecycle Management

- All users must have a unique, auditable ID assigned via the Identity Management System (IMS) (AC-2).
- Creation, modification, and deletion of accounts must follow documented provisioning workflows (AC-2, PS-3).
- Temporary accounts (e.g., vendors or interns) must have automatic expiry dates assigned at creation.

2.1.3.2 Authentication and MFA

- Multi-Factor Authentication (MFA) is mandatory for:
  - All remote access (VPN, cloud consoles)
  - All privileged accounts (admins, DevOps, security team)
  - GitHub, Jira, AWS root accounts, Azure AD portal (IA-2(1), IA-2(2))
- Only hardware keys or company-approved authenticators (e.g., Microsoft Authenticator, Duo) may be used.

2.1.3.3 Authorization and Access Control

- Access must follow the principle of least privilege and be enforced through Role-Based Access Control (RBAC) (AC-6).
- Department managers must approve all access change requests.
- Access to the following resources is considered privileged:
  - Firmware repositories
  - Cloud environments
  - Licensing database
  - Telemetry pipelines

2.1.3.4 Session Management and Timeout Controls

- Admin interfaces must auto-logout after 10 minutes of inactivity.
- Console sessions must be limited to 1 hour with enforced reauthentication (AC-12, AC-11).

2.1.3.5 Privileged Account Management

- Shared accounts are prohibited unless formally justified, approved by the CISO, and auditable (AC-2(9)).
- Privileged accounts must be reviewed monthly by the IT Security Team.
- Privileged access use must be logged and reviewed via SIEM (AU-2).

2.1.3.6 Endpoint Device Access

- USB ports must be locked via MDM unless using the approved ViraShield Portable AV.
- Workstations and laptops must authenticate USB AV devices before usage.

2.1.3.7 Access Reviews and Termination

- Quarterly access reviews are mandatory for all business units.
- Departing employees' accounts must be disabled within 2 hours of HR offboarding notice.
- Admin access must be removed immediately upon notice of resignation or termination.

2.1.4 Roles and responsibilities

- **CISO** – Ensures policy compliance and continuous alignment with NIST and ISO frameworks
- **IT Security Team** – Implements and maintains IAM infrastructure, conducts access reviews and logs
- **HR Department –** Initiates identity workflows upon onboarding/offboarding
- **Department Managers –** Approve access requests and validate role-to-permission alignment
- **End Users** – Maintain security of credentials, report anomalies or unauthorized access

2.1.5 Enforcement

Failure to comply with this policy may result in access revocation, disciplinary actions up to and including termination, and legal consequences depending on severity. Security violations may be reported to legal, HR, or regulatory bodies as required.

2.1.6 Reference

- NIST SP 800-53 Rev. 5: AC-1 to AC-17, IA-2
- ISO/IEC 27001:2022 – Annex A.5: Access Control
- ViraShield Secure Development Policy
- ViraShield USB Device Security Policy
- ViraShield Data Classification Standard

2.2 Acceptable Use Policy

Frameworks: NIST SP 800-53 (PL-4), ISO/IEC 27001:2022 (Annex A.5)

Policy #: VS-AUP-002

Policy Title: Acceptable Use Policy

Policy Owner: Information Security Manager

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Mandatory

2.2.1 Purpose

To establish clear rules and responsibilities for the appropriate use of ViraShield Technologies Inc.'s systems, services, and digital assets by employees, contractors, and partners. This policy ensures that resources are used securely, ethically, and in a way that supports business operations while reducing the risk of data loss, unauthorized access, or reputational damage.

2.2.2 Scope

This policy applies to:

- All ViraShield personnel, contractors, interns, and third-party vendors
- All computing and communications equipment including company-issued laptops, desktops, mobile phones, and USB antivirus devices
- All services including internal software (Slack, Jira, GitHub), cloud environments, VPN, remote work solutions, and physical devices issued or connected to company infrastructure

2.2.3 Policy Statement

2.2.3.1 Authorized Use

- Company systems must be used for business-related activities only.
- Personal use must not interfere with business functions or compromise security.
- Devices may not be used for accessing or distributing offensive, illegal, or non-business-related content.

2.2.3.2 Device and Network Usage

- Users must not install unauthorized software, modify configurations, or bypass company security settings.
- Unauthorized USB storage/media devices are prohibited; only ViraShield-approved USB AV products may be used.

- VPN must be used when connecting remotely to any internal resource.

2.2.3.3 Data Protection

- Sensitive information must not be transferred or stored on personal cloud services.
- Emailing company IP, source code, or telemetry logs to external accounts is strictly prohibited.
- Systems must be locked when unattended, and devices must be physically secured.

2.2.3.4 Communication

- All company communications must be professional and respectful.
- Use of anonymous browsing tools (VPNs, Tor, proxies) is prohibited unless explicitly authorized.
- All corporate communications (email, Slack, Confluence) are monitored in accordance with internal policy.

2.2.3.5 Monitoring and Auditing

- All activities on ViraShield systems are subject to logging and audit.
- IT Security may review logs to investigate policy violations or suspicious behavior.

2.2.4 Roles and responsibilities

- **Information Security Manager** – Policy enforcement, annual review, and updates
- **IT Department** – Enforces device restrictions, VPN requirements, and monitors system logs
- **HR and Managers** – Ensure that users sign and understand the Acceptable Use Policy upon hiring
- **Employees and Contractors –** Comply with this policy and report any misuse

2.2.5 Enforcement

Violations of this policy will result in disciplinary action up to and including termination of employment or contract. Unauthorized activity may result in legal action if regulatory or criminal thresholds are crossed.

2.2.6 Reference

- NIST SP 800-53 Rev. 5: PL-4
- ISO/IEC 27001:2022 – Annex A.5
- ViraShield Code of Conduct

- ViraShield Remote Work Security Policy
- ViraShield Internet Use Monitoring Standard

2.3 Remote Work Security Policy

Frameworks: NIST SP 800-46, ISO/IEC 27001:2022 (Annex A.6)

Policy #: VS-RWP-003

Policy Title: Remote Work Security Policy

Policy Owner: Information Security Manager

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Mandatory

2.3.1 Purpose

To define the necessary technical, physical, and administrative controls required for secure remote work across ViraShield Technologies Inc. This policy mitigates the increased risks associated with remote access, mobile devices, and off-premises work environments.

2.3.2 Scope

This policy applies to:

- All ViraShield employees, contractors, interns, and vendors working remotely (full-time or hybrid)
- All devices used to access company systems remotely, including laptops, tablets, mobile phones, and USB-based AV devices
- All remote access solutions, including VPN, cloud portals, mobile device management (MDM), and video conferencing platforms (e.g., Zoom, Microsoft Teams)

2.3.3 Policy Statement

2.3.3.1 Remote Access Controls

- Access to internal systems must be made only through the company-managed VPN solution with MFA enabled.
- Remote connections must use encrypted channels (TLS 1.3 minimum) and adhere to company network segmentation protocols.
- Cloud-based admin consoles must restrict login to pre-approved geographic locations and IP addresses.

2.3.3.2 Device Security Requirements

- All remote devices must:
  - Be enrolled in ViraShield's MDM platform
  - Run approved antivirus software with up-to-date threat definitions
  - Have full-disk encryption enabled (e.g., BitLocker, FileVault)
  - Be password-locked after 5 minutes of inactivity
- Personal devices (BYOD) are prohibited unless explicitly approved and onboarded by IT.

2.3.3.3 USB and Peripheral Usage

- Only approved USB AV products issued by ViraShield may be used in remote work environments.
- Unauthorized USB storage or peripheral devices are blocked by endpoint controls.
- USB activity logs must be retained and reviewed monthly.

2.3.3.4 Communication

- Employees must:
  - Use private, secure Wi-Fi networks only (no public access points)
  - Lock screens when stepping away from devices
  - Avoid discussing sensitive information in shared or public environments
  - Use privacy filters when working in public spaces

2.3.3.5 Data Handling and Storage

- Remote users must not store company IP, telemetry logs, or customer data on local drives.
- All document collaboration must occur via authorized cloud storage (e.g., SharePoint, OneDrive).
- Remote workers must not print confidential information unless approved by management.

2.3.3.6 Incident Response Requirements

- Any security incident, including device theft, unauthorized access, or suspicious system behavior, must be reported to the IT Security team within 30 minutes.
- Remote workers must cooperate fully with digital forensic investigations and remote wipe procedures if needed.

2.3.4 Roles and responsibilities

- **Information Security Manager** – Maintains and enforces remote work security policy and procedures
- **IT Security Team** – Implements technical controls, MDM configuration, and access monitoring
- **Department Managers** – Approve remote work status and ensure employees comply with controls
- **Employees and Contractors** – Ensure their remote environments adhere to all security requirements

2.3.5 Enforcement

Any user found in violation of this policy may face disciplinary action, including but not limited to revocation of remote access privileges, termination of employment or contract, and potential legal action depending on the severity of the breach.

2.3.6 Reference

- NIST SP 800-46: Guide to Enterprise Telework, Remote Access, and BYOD Security
- ISO/IEC 27001:2022 – Annex A.6: Organizational Controls
- ViraShield Acceptable Use Policy
- ViraShield Mobile Device Management (MDM) Configuration Standard
- ViraShield Secure Remote Access Procedure
- ViraShield Internet Use Monitoring Standard

2.4 Employee Onboarding & Offering Policy

Frameworks: NIST SP 800-53 (PS-3, PS-4), ISO/IEC 27001:2022 (Annex A.7)

Policy #: VS-EOO-004

Policy Title: Employee Onboarding & Offboarding Policy

Policy Owner: Human Resources Director

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Mandatory

2.4.1 Purpose

To define a standardized and secure approach to onboarding new personnel and offboarding departing individuals, ensuring timely provisioning and deprovisioning of system access, data handling responsibilities, and compliance with organizational security practices.

2.4.2 Scope

This policy applies to:

- All new hires, contractors, vendors, and temporary staff joining or leaving ViraShield Technologies Inc.
- All departments responsible for user identity, access rights, and HR coordination
- All IT-managed systems including email, VPN, collaboration tools, source code repositories, and customer data portals

2.4.3 Policy Statement

2.4.3.1 Onboarding Procedures

- HR must initiate a formal onboarding ticket in the Identity Management System (IMS) at least 3 business days before a new hire’s start date.
- Access rights must align strictly with the employee’s job role, approved by their department manager and verified by IT Security.
- Mandatory onboarding training (including AUP, Remote Work Policy, and Data Handling) must be completed within the first 5 business days.

2.4.3.2 Account Provisioning and Access Control

- New employees are granted access only to systems necessary for their role using RBAC principles.
- Privileged access (e.g., to source code or telemetry data) requires approval from both the CISO and relevant department head.
- A unique company ID and email must be assigned, along with initial temporary credentials that require password reset upon first use.

2.4.3.3 Asset Allocation

- IT must provide and track company-issued hardware (e.g., laptops, USB AV devices, access tokens) via the asset management system.
- Devices must be preconfigured with security baselines, VPN profiles, and company antivirus.

2.4.3.4 Offboarding Procedures

- Department managers or HR must notify IT and Security at least 5 business days in advance of a scheduled termination or immediately upon an unplanned departure.
- All system access must be disabled within 2 hours of separation.

- Physical devices must be returned and verified before final payroll release.

2.4.3.5 Exit Review and Data Sanitization

- IT must conduct an exit access audit to ensure all user credentials, tokens, and system permissions have been revoked.
- Returned devices must undergo secure wipe procedures in accordance with the Data Sanitization Policy.
- Departing personnel must be reminded of any continuing obligations (e.g., NDA, IP rights) in their exit interview.

2.4.4 Roles and responsibilities

- **Human Resources Director** – Coordinates onboarding/offboarding tasks with departments and ensures policy adherence
- **IT Department** – Manages access provisioning, asset delivery, and credential revocation
- **Information Security Team** – Verifies access levels, logs all changes, and performs final offboarding audits
- **Department Managers** – Approve role-based access and notify HR and IT of personnel changes

2.4.5 Enforcement

Any failure to comply with this policy—such as delayed access revocation or improper equipment return—may result in administrative penalties or risk assessment review. Security breaches tied to noncompliance may trigger disciplinary action or legal proceedings.

2.4.6 Reference

- NIST SP 800-53: PS-3 (Personnel Screening), PS-4 (Personnel Termination)
- ISO/IEC 27001:2022 – Annex A.7: People Controls
- ViraShield Identity and Access Management Policy
- ViraShield Acceptable Use Policy
- ViraShield Data Sanitization Standard

2.5 Insider Threat Detection Policy

Frameworks: NIST SP 800-53 (CM-3, SI-4), CERT Insider Threat Guide

Policy #: VS-ITD-005

Policy Title: Insider Threat Detection Policy

Policy Owner: Chief Information Security Officer (CISO)

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Confidential

2.5.1 Purpose

To establish procedures and controls for detecting, mitigating, and responding to insider threats—whether intentional or accidental—originating from current or former employees, contractors, or trusted third-party vendors with access to ViraShield assets.

2.5.2 Scope

This policy applies to:

- All full-time, part-time, temporary, and contract personnel
- All physical and logical access to company systems, source code, infrastructure, USB antivirus firmware, and telemetry data
- Internal teams including R&D, QA, Cloud Security, Support, and Licensing Ops

2.5.3 Policy Statement

2.5.3.1 Insider Threat Program

- ViraShield shall maintain an Insider Threat Program (ITP) led by the CISO with cross-functional membership (HR, Legal, Security, and IT).
- The ITP must perform annual insider threat risk assessments and coordinate investigations.

2.5.3.2 Baseline Behavior and Monitoring

- Security baselines shall be defined per role (e.g., developer, DevOps, support agent) using UEBA (User and Entity Behavior Analytics).
- Deviations from expected behavior such as unusual access times, data exports, or USB insertions shall be flagged automatically.

2.5.3.3 Access Control and Least Privilege

- Access must align with job responsibilities (RBAC) and be reviewed quarterly.
- High-risk data (firmware, AI models, license keys) must be access-logged and cryptographically validated (NIST CM-3).

2.5.3.4 Logging and Continuous Monitoring

- All administrative, codebase, and cloud infrastructure access must be monitored using the SIEM platform.

- Security Intelligence (SI-4) rules must detect privilege escalation, exfiltration patterns, and sudden access anomalies.

2.5.3.5 Anonymous Reporting

- Employees must have secure and anonymous channels to report insider threats without fear of retaliation.
- All reports are logged, triaged, and escalated according to severity and risk level.

2.5.3.6 Incident Handling and Forensics

- Detected insider threat incidents must follow the Incident Response Policy (VS-IRP-006).
- Devices involved shall be isolated, imaged, and examined by forensic analysts.
- HR and Legal must be involved if termination, criminal referral, or civil litigation is warranted.

2.5.4 Roles and responsibilities

- **CISO** – Owns the Insider Threat Program and ensures alignment with NIST/CERT best practices
- **Security Operations Team** – Implements UEBA tools and analyzes behavioral anomalies
- **HR & Legal** – Participate in response procedures and ensure legal compliance
- **Department Managers** – Ensure employees only access required systems
- **All Staff** – Report suspicious behavior and comply with data access protocols

2.5.5 Enforcement

Violations or confirmed insider threats will result in immediate access revocation, potential employment termination, legal action, and reporting to law enforcement or regulatory authorities as appropriate.

2.5.6 Reference

- NIST SP 800-53 Rev. 5: CM-3 (Configuration Change Control), SI-4 (System Monitoring)
- CERT Guide to Insider Threat Programs
- ViraShield Incident Response Policy
- ViraShield Access Control and Logging Policy
- ViraShield Behavioral Analytics Guidelines

3 Firmware & Product Development Policies

3.1 Firmware Integrity and Code Signing Policy

Frameworks: NIST SP 800-147, ISO/IEC 27001:2022 (Annex A.8)

Policy #: VS-FIC-006

Policy Title: Firmware Integrity and Code Signing Policy

Policy Owner: Director of Embedded Systems Security

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Confidential

3.1.1 Purpose

This policy ensures the confidentiality, integrity, and authenticity of firmware distributed with ViraShield devices. It establishes the mandatory processes and controls for cryptographic code signing, secure boot validation, version control, unauthorized modification prevention, and rollback safety. This policy protects against supply chain tampering, firmware malware injection, and unauthorized firmware execution.

3.1.2 Scope

This policy applies to all firmware developed, modified, or deployed for the ViraShield Portable AV product line. It includes:

- All firmware codebases and associated binaries
- Build pipelines (CI/CD) and artifact repositories
- Firmware signing tools and key management systems
- OTA (Over-the-Air) update mechanisms
- All engineering teams involved in embedded development, QA, operations, and security compliance

3.1.3 Policy Statement

3.1.3.1 Firmware Build and Signing Standards

- All firmware must be compiled using ViraShield's designated secure build environment.
- The final binary must be signed using FIPS 140-3 compliant algorithms (e.g., ECDSA, RSA-4096) before it is eligible for release.

- Signing keys must be stored in an HSM (Hardware Security Module) with role-based access control (RBAC) enforced. Only CI/CD build agents and authorized signers may access the signing function.
- Every signed image must include a cryptographic signature block that includes a hash, signature, timestamp, and firmware version ID.

3.1.3.2 Secure Boot and Runtime Validation

- All ViraShield AV devices must verify firmware signatures at boot using a Secure Boot mechanism (in accordance with NIST SP 800-147).
- If validation fails:
  - The device will refuse to boot the unsigned or tampered firmware.
  - A telemetry alert will be sent if internet is available.
  - The device will enter a safe diagnostic mode until a valid firmware is re-flashed.
- The root-of-trust must begin with an immutable bootloader stored in read-only memory (ROM).

3.1.3.3 Firmware Versioning and Traceability

- Each firmware release must be assigned a unique version ID and changelog entry.
- Firmware source code commits must be traceable to specific Jira tickets and developer approvals.
- All build artifacts must be logged in an immutable audit log system (GitLab CI/CD or equivalent).

3.1.3.4 Code Review and Vulnerability Testing

- Prior to signing, all firmware updates must:
- Undergo a formal peer code review
- Pass automated static and dynamic vulnerability scanning
- Be tested against ViraShield’s hardware emulation platform and physical QA test rigs
- QA must approve the test suite before forwarding the build for signature.

3.1.3.5 OTA Firmware Distribution

- Firmware must be delivered to devices using ViraShield’s secure OTA channel:
- Encrypted using TLS 1.3

- Signed payloads must include firmware hash, manifest, and expiration timestamp
- OTA servers will reject update requests from devices that are not compliant with minimum firmware version or licensing status.

3.1.3.6 Unauthorized Firmware Detection and Rollback

- Devices must reject any firmware that:
- Lacks a valid signature
- Has an expired or revoked signing certificate
- Does not match expected product ID or region lock
- The Firmware Revocation List (FRL) is stored locally and updated via OTA.
- Rollback requests must only occur through signed, validated images from a trusted update server.

3.1.4 Roles and responsibilities

- **Director of Embedded Systems Security** – Owns this policy and ensures all firmware security measures meet NIST and ISO standards.
- **Firmware Development Team** – Implements and documents firmware changes, submits builds for review and signing.
- **DevSecOps Team** – Manages secure CI/CD, HSM key protection, signing services, and build artifact logging.
- **Quality Assurance Team** – Verifies firmware behavior on physical and emulated devices, performs vulnerability checks.
- **Manufacturing and Production** – Flashes signed firmware only and confirms secure boot behavior during device testing.

3.1.5 Enforcement

Violations of this policy—such as bypassing signing processes or releasing unsigned firmware—are considered critical security infractions. Offenders may face suspension, termination, and possible legal action. All firmware releases must follow the verified signing and QA process outlined above.

3.1.6 Reference

- NIST SP 800-147: BIOS Protection Guidelines
- ISO/IEC 27001:2022 – Annex A.8: Secure Development
- ViraShield Secure OTA Update Policy

- ViraShield CI/CD Build Pipeline Security Standard
- ViraShield Rollback and Firmware Revocation Controls

3.2 Secure Code Development Policy

Frameworks: NIST SP 800-53 (SA-11), OWASP SAMM, NIST SSDF

Policy #: VS-SCD-007

Policy Title: Secure Code Development Policy

Policy Owner: Director of Application Security

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Confidential

3.2.1 Purpose

The purpose of this policy is to ensure that all software and firmware developed by ViraShield Technologies Inc. follows secure development practices throughout its lifecycle. This includes secure coding standards, vulnerability detection, code reviews, dependency validation, and continuous security testing. The policy is intended to reduce the risk of security vulnerabilities in production systems and to maintain compliance with industry frameworks.

3.2.2 Scope

This policy applies to:

- All ViraShield-developed software and firmware including embedded code for AV USB devices.
- Development teams working on mobile apps, firmware, server-side services, AI models, OTA systems, licensing systems, and update agents.
- All code repositories (GitHub Enterprise, GitLab), build pipelines, libraries, and third-party components used in product development.

3.2.3 Policy Statement

3.2.3.1 Secure Coding Standards

- All developers must adhere to secure coding standards such as OWASP Secure Coding Practices and SEI CERT C/C++ guidelines (where applicable).
- Secure code guidelines must be reviewed and updated at least annually by the AppSec team.

- Language-specific checklists and patterns (e.g., for C, Python, JavaScript, Rust) must be documented.

3.2.3.2 Code Reviews and Approval

- Peer code reviews are mandatory for all commits pushed to protected branches.
- Code reviews must include security-focused checkpoints (e.g., input validation, cryptographic use, access controls).
- No code shall be merged without approval from a senior developer or AppSec designee.

3.2.3.3 Static and Dynamic Analysis

- All code must pass static analysis (SAST) using approved tools (e.g., SonarQube, Fortify, CodeQL).
- Dynamic scanning (DAST) shall be applied to running builds and staging environments.
- Critical vulnerabilities identified must be remediated prior to release; high/medium findings require documented mitigation.

3.2.3.4 Dependency and Third-party Library Management

- Third-party dependencies must be vetted and monitored using SBOM (Software Bill of Materials) tools.
- Packages must be verified for license compliance, known vulnerabilities (CVEs), and supply chain risks.
- Only components from approved registries or repositories may be used.

3.2.3.5 Secure Build Pipelines

- CI/CD pipelines must:
  - Enforce branch protections and build validations
  - Automatically scan for secrets, malware, and misconfigurations
  - Log all build actions in an immutable audit trail
- Build artifacts must be cryptographically signed before deployment to QA or production.

3.2.3.6 Training and Awareness

- Developers must complete secure coding training annually.
- AppSec must deliver periodic workshops on emerging threats (e.g., supply chain attacks, LLM-specific vulnerabilities).

- Newly onboarded engineers must complete secure development orientation within 10 days.

3.2.3.7 Secure Firmware Development Practices

- Firmware code (C/C++/Assembly) must follow memory safety best practices (e.g., stack protections, buffer limits).
- Cryptographic APIs must be used via vetted libraries only (e.g., OpenSSL FIPS mode, BoringSSL).
- Dangerous compiler flags or deprecated APIs must be restricted at the build level.

3.2.4 Roles and responsibilities

- **Director of Application Security** – Owns this policy and oversees its implementation across all teams.
- **AppSec Team** – Maintains secure coding standards, performs static/dynamic scans, and approves exceptions.
- **Development Leads** – Ensure secure development principles are enforced in sprint planning and reviews.
- **Developers** – Write secure code, complete required training, and participate in secure peer reviews.
- **DevOps Engineers** – Maintain secure CI/CD pipelines and monitor integrity of builds and signing workflows.

3.2.5 Enforcement

Non-compliance with secure coding requirements or use of unauthorized dependencies will result in immediate rejection of the affected codebase or build. Repeat violations may result in loss of merge privileges, reassignment, or disciplinary action depending on the severity.

3.2.6 Reference

- NIST SP 800-53 Rev. 5: SA-11 (Developer Security Testing and Evaluation)
- NIST Secure Software Development Framework (SSDF) v1.1
- OWASP Software Assurance Maturity Model (SAMM)
- OWASP Secure Coding Practices Quick Reference
- ViraShield Firmware Development Standards
- ViraShield CI/CD Pipeline Security Requirements

3.3 Intellectual Property Protection Policy

Frameworks: NIST SP 800-53 (PL-8), ISO/IEC 27001:2022 (Annex A.8)

Policy #: VS-IPP-008

Policy Title: Intellectual Property Protection Policy

Policy Owner: Chief Legal & Compliance Officer

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Confidential

3.3.1 Purpose

The purpose of this policy is to establish controls that protect the intellectual property (IP) assets of ViraShield Technologies Inc., including proprietary firmware, detection algorithms, subscription logic, design documentation, source code, and licensing systems. This policy ensures the confidentiality, integrity, and legal enforceability of ViraShield's IP, while complying with contractual, regulatory, and security obligations.

3.3.2 Scope

This policy applies to:

- All ViraShield employees, contractors, and partners who access, develop, maintain, or distribute IP-bearing materials.
- All systems and repositories where IP is stored, including GitHub Enterprise, CI/CD platforms, OTA firmware infrastructure, and AI/ML model archives.
- All phases of product development, testing, documentation, marketing, and licensing operations.

3.3.3 Policy Statement

3.3.3.1 Secure Definition of Protected IP

- ViraShield considers the following assets as protected IP:
  - Embedded firmware for AV USB devices
  - Proprietary malware detection heuristics and AI models
  - Subscription licensing engine and product activation logic
  - Threat telemetry processing and signature update algorithms
  - Brand assets, hardware design schematics, UX flows, and internal product documentation

3.3.3.2 Access Control to IP Address

- IP assets must be stored in secure, access-controlled environments using RBAC and MFA.
- Source code repositories must restrict write access to designated developers and be reviewed before merges.
- Legal or compliance staff must review third-party access requests involving IP (e.g., vendors, auditors)

3.3.3.3 Non-Disclosure and Confidentiality Obligations

- All personnel must sign binding Non-Disclosure Agreements (NDAs) prior to receiving access to protected materials.
- Departing employees must participate in an IP exit briefing confirming ongoing obligations under NDA, IP assignment, and non-compete clauses.

3.3.3.4 Licensing and Attribution Control

- All outbound code, libraries, and product documents must be reviewed for proprietary vs. open-source components.
- Public release of software, marketing content, or firmware must be authorized by Legal and AppSec.
- IP ownership must be asserted clearly in device firmware headers, splash screens, or licensing dialogs.

3.3.3.5 Monitoring and Data Loss Prevention

- IP-related directories and tools must be monitored by DLP systems for unauthorized transfer attempts.
- External drive usage, Git clone volume, and outbound data size anomalies must trigger alerts.
- Exfiltration attempts must follow the Insider Threat Detection and Incident Response procedures.

3.3.3.6 Contractual and Regulatory Compliance

- The IP protection program must align with global data protection frameworks (e.g., GDPR, CCPA), software export laws (e.g., EAR), and ISO 27001 control expectations.
- Annual audits of IP controls and inventory must be performed and documented for compliance and legal readiness.

3.3.4 Roles and responsibilities

- **Chief Legal & Compliance Officer –** Owns this policy and enforces legal protections for company IP across geographies.
- **Director of Embedded Systems Security** – Ensures firmware, OTA, and product logic IP is protected during design, deployment, and updates.
- **Software Development Teams** – Responsible for securing source code and submitting IP documentation where required.
- **IT Security & DevSecOps Teams –** Enforce RBAC, secure repositories, monitor for unauthorized access or exfiltration.
- **HR Department** – Ensures all new hires and departing personnel acknowledge IP ownership and confidentiality obligations.

3.3.5 Enforcement

Violations of IP protection standards may result in disciplinary action, termination, legal action, and criminal prosecution where applicable. Attempted or actual theft, leakage, or sabotage of ViraShield intellectual property is considered a severe offense and is grounds for immediate escalation and litigation.

3.3.6 Reference

- NIST SP 800-53 Rev. 5: PL-8 (Information Security Architecture – Intellectual Property Protection)
- ISO/IEC 27001:2022 – Annex A.8: Secure Development and IP Control
- ViraShield NDA & IP Assignment Agreement
- ViraShield Insider Threat Detection Policy
- ViraShield Source Code Repository Access Policy

3.4 Device Hardening Policy

Frameworks: NIST SP 800-53 (CM-6), NIST IoT Guidelines

Policy #: VS-DHP-009

Policy Title: Device Hardening Policy

Policy Owner: Director of Embedded Systems Security

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Confidential

3.4.1 Purpose

The purpose of this policy is to define the baseline hardening standards for all ViraShield hardware devices to prevent unauthorized access, tampering, exploitation, or modification. This includes pre-production, production, and deployed USB-based antivirus hardware. The policy enforces secure default configurations, disables unnecessary functions, ensures protection against firmware manipulation, and aligns with NIST guidance on device cybersecurity.

3.4.2 Scope

This policy applies to:

- All USB-based ViraShield Portable AV products, including both USB-A and USB-C variants.
- Embedded firmware, bootloaders, physical interfaces, and device-level security controls.
- Engineering, firmware, QA, production, and DevSecOps teams involved in designing, testing, and deploying hardened devices.

3.4.3 Policy Statement

3.4.3.1 Secure Default Configuration

- Devices must ship with the most restrictive configuration as the default.
- All ports, communication channels, debug interfaces, or hardware features not explicitly required for device operation must be disabled or physically fused off.
- The default operating mode must require no external configuration by the user.

3.4.3.2 Firmware and Bootloader Hardening

- Bootloaders must use Secure Boot with digital signature enforcement as per the Firmware Integrity Policy.
- Firmware must:
- Disable all debug symbols, backdoors, and development keys before release.
- Be protected against unauthorized overwrite using write-protect and OTP (One-Time Programmable) flags.
- Implement firmware version lock to prevent downgrading unless cryptographically approved.

3.4.3.3 Physical Security Controls

- Devices must be manufactured using tamper-evident and tamper-resistant casing (e.g., epoxy coating, ultrasonic welding).
- Sensitive chips and components must be protected from side-channel attacks (e.g., decapsulation, fault injection) via hardware layout obfuscation and shielding.
- Serial interfaces (UART, JTAG) must be permanently disabled or require hardware-level cryptographic challenge-response.

3.4.3.4 Cryptographic Enforcement

- All communications (e.g., OTA updates, cloud sync, license validation) must enforce TLS 1.3 with strict certificate pinning.
- Devices must include a factory-programmed unique cryptographic key pair stored in a secure enclave or TPM.

3.4.3.5 Unused Features and Services

- IP-related Any non-operational protocols (e.g., Wi-Fi, BLE, unused USB class descriptors) must be removed or disabled.
- The device must not expose any unnecessary USB interfaces or appear as mass storage unless explicitly required.

3.4.3.6 Contractual and Regulatory Compliance

- The IP protection program must align with global data protection frameworks (e.g., GDPR, CCPA), software export laws (e.g., EAR), and ISO 27001 control expectations.
- Annual audits of IP controls and inventory must be performed and documented for compliance and legal readiness.

3.4.3.7 Hardening Verification and Audits

- All hardened firmware builds must undergo binary analysis, fuzz testing, and penetration testing before release.
- Hardware review checklists must be signed off by both firmware and security leads before final production.
- Random samples from manufacturing must be tested for bypass or modification vulnerabilities before shipment.

3.4.4 Roles and responsibilities

- **Director of Embedded Systems Security** – Owns and enforces hardening controls across all hardware and firmware.

- **Firmware Engineering Team** – Implements secure configuration defaults and validates runtime protections.
- **Hardware Design & Manufacturing** – Designs tamper-resistant enclosures and disables unused interfaces.
- **Quality Assurance (QA)** – Tests hardened devices for bypass attempts and conformance to release hardening checklist.
- **DevSecOps Team** – Verifies post-build firmware binaries, automates device validation pipeline checks.

3.4.5 Enforcement

Any deviation from this hardening policy during development, testing, or manufacturing may result in release suspension, device recall, or escalation to the Chief Information Security Officer. Unauthorized modification of hardened devices in the field constitutes a violation of IP protection and security assurance obligations.

3.4.6 Reference

- NIST SP 800-53 Rev. 5: CM-6 (Configuration Settings)
- NIST IR 8259A: Core Baseline for IoT Device Cybersecurity
- NIST IR 8259B: Manufacturer Usage Description (MUD)
- ISO/IEC 27001:2022 Annex A.8: Secure Development
- ViraShield Firmware Integrity and Code Signing Policy (3.1)
- ViraShield OTA Update Validation Policy (11.2)

3.5 Third-party Component Validation Policy

Frameworks: NIST SP 800-53 (SA-12), ISO/IEC 27001:2022 (Annex A.15)

Policy #: VS-TPC-010

Policy Title: Third-party Component Validation Policy

Policy Owner: Director of Supply Chain Security

Approval Date: March 28, 2025

Review Date: March 28, 2026

Policy Classification: Internal – Confidential

3.5.1 Purpose

The purpose of this policy is to ensure that all third-party components—hardware, software, firmware, and services—integrated into ViraShield's products or infrastructure are vetted, validated, and continuously monitored for security, legal compliance, and operational integrity. This is vital to mitigating supply chain risk and aligning with global standards for secure development and supplier assurance.

3.5.2 Scope

This policy applies to:

- All third-party libraries, modules, and firmware integrated into the ViraShield Portable AV product.
- Open-source packages, SDKs, external APIs, and cloud-hosted services.
- Hardware components procured from external vendors (e.g., chipsets, memory, USB controllers).
- Any third-party code, infrastructure tools, or manufacturing firmware used in testing, OTA delivery, or device configuration.

3.5.3 Policy Statement

3.5.3.1 Supplier Assessment and Due Diligence

- All vendors must undergo a risk-based supplier assessment before contract execution.
  - Assessment includes:
  - Vendor security practices
  - Data handling procedures
  - Legal ownership and licensing of the component
  - Past security incidents or CVEs associated with their products
- Vendors handling sensitive data or code must sign security addendums and NDA agreements.

3.5.3.2 Component Inventory and SBOM

- A Software Bill of Materials (SBOM) must be maintained for all third-party components used in firmware and infrastructure.
- The SBOM must include:
  - Package name and version
  - Source repository and license
  - CVE status and mitigation notes
  - Validation date and approver

3.5.3.3 Code Scanning and Validation

- All third-party libraries must undergo:

  - Static code analysis (if source is available)
  - Malware scanning and behavior testing (for binaries)
  - License validation (e.g., GPL, MIT, Apache 2.0)
- High-risk components must be sandboxed or isolated in runtime environments.

3.5.3.4 Firmware and Hardware Component Verification

- All hardware suppliers must provide:
  - Chain of custody documents
  - Firmware hashes or signed binaries for secure boot validation
  - Physical tamper resistance certification (when applicable)
- Firmware from external suppliers must be signed and verified before flashing on devices.

3.5.3.5 Ongoing Monitoring and Remediation

- Component versions must be monitored for new vulnerabilities (e.g., via NVD, GitHub security advisories).
- Security alerts must trigger an impact assessment and remediation plan within 7 business days.
- Retired or unmaintained third-party components must be deprecated from the production pipeline.

3.5.4 Roles and responsibilities

- **Director of Supply Chain Security** – Owns this policy and coordinates all supplier risk and validation activities.
- **Procurement Department –** Performs vendor intake, maintains supplier records, and ensures contracts include security clauses.
- **DevSecOps & AppSec Teams –** Scan, analyze, and approve third-party code before integration.
- **QA and Firmware Teams –** Validate hardware drivers, embedded binaries, and component interactions.
- **Legal and Compliance –** Ensure license compatibility and contract enforcement with third-party vendors.

3.5.5 Enforcement

No unvetted third-party component may be deployed into production systems or firmware. Violations—such as bypassing validation, using non-compliant licenses, or sourcing from non-approved vendors—will result in immediate rollback, internal investigation, and potential disciplinary action.

3.5.6 Reference

- NIST SP 800-53 Rev. 5: SA-12 (Supply Chain Protection)
- ISO/IEC 27001:2022 – Annex A.15: Supplier Relationships
- ViraShield Secure Build Policy
- ViraShield Firmware Release Checklist
- OWASP CycloneDX SBOM Standard
- ViraShield Vendor Risk Assessment Template

4 Customer Data & Privacy Policies

4.1 Privacy and Telemetry Consent Policy

Frameworks: NIST SP 800-53 (AP-1), GDPR, ISO/IEC 27701

Policy #: VS-PTC-011

Policy Title: Privacy and Telemetry Consent Policy

Policy Owner: Data Protection Officer (DPO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: External – Public & Regulatory

4.1.1 Purpose

The purpose of this policy is to ensure lawful, transparent, and secure processing of user data collected through ViraShield devices and services. This includes all telemetry, threat intelligence, subscription-related data, and voluntary diagnostic logs gathered during the operation of ViraShield Portable AV products. The policy enforces user consent management, aligns with global privacy regulations, and safeguards personal and system-level metadata.

4.1.2 Scope

This policy applies to:

- All customers using ViraShield Portable AV products or connected licensing and update services.
- All data processed by telemetry modules, including:
  - Threat detection metadata

  - Device fingerprinting
  - Subscription usage logs
- Backend systems, cloud endpoints, and secure storage used to process or analyze telemetry.

4.1.3 Policy Statement

4.1.3.1 Consent-Based Collection

- All Telemetry and personal data must only be collected with **explicit, opt-in consent** from the user.
- Consent prompts must:
  - Clearly state what data will be collected
  - Explain the purpose (e.g., threat research, product improvement)
  - Provide options to accept, decline, or configure scope of collection

4.1.3.2 Types of Data Collected

- The following data may be collected only with consent:
  - Anonymized threat signatures or scan results
  - OS type, device model, and firmware version
  - Subscription activation timestamps and region
  - Diagnostic logs related to false positives or hardware issues

4.1.3.3 Firmware Versioning and Traceability

- Personally Identifiable Information (PII) must be redacted or anonymized at source unless otherwise authorized by the user.
- Aggregated telemetry must not be re-identifiable and must follow ISO 27701 principles.

4.1.3.4 Data Anonymization and Aggregation

- Prior Personally Identifiable Information (PII) must be redacted or anonymized at source unless otherwise authorized by the user.
- Aggregated telemetry must not be re-identifiable and must follow ISO 27701 principles.

4.1.3.5 Right to Withdraw Consent

- Firmware Users can revoke telemetry consent at any time through:
  - Device UI prompts
  - ViraShield support portal

- Consent changes must take effect within 24 hours and be reflected in backend systems.

4.1.3.6 Storage and Retention

- All telemetry data must be encrypted in transit and at rest (TLS 1.3 and AES-256).
- Data retention is limited to:
  - 90 days for raw telemetry
  - 12 months for aggregated, non-identifiable research logs
- Upon consent withdrawal or product unregistration, all identifiable logs must be deleted within 30 days.

4.1.3.7 Regional Data Handling (GDPR / APAC)

- All For users in the EU, Singapore, and India:
  - Consent records must be logged with timestamp and consent version.
  - All processing must occur on region-local infrastructure unless explicitly consented otherwise.
- GDPR Articles 6, 7, and 25 apply.

4.1.4 Roles and responsibilities

- **Data Protection Officer (DPO) –** Maintains this policy, audits consent records, and serves as the contact point for regulatory inquiries.
- **Cloud Engineering Team –** Implements data separation, secure storage, and encryption measures for telemetry.
- **Customer Support Team –** Manages user consent requests, withdrawals, and data deletion processes.
- **Legal & Compliance –** Ensures compliance with GDPR, ISO 27701, and global privacy obligations.

4.1.5 Enforcement

Any unauthorized collection, storage, or processing of telemetry or personal data will result in immediate suspension of access to processing systems and possible disciplinary action, including legal consequences. ViraShield reserves the right to disable product features pending consent violations.

4.1.6 Reference

- NIST SP 800-53 Rev. 5: AP-1 (Authority to Process Personally Identifiable Information)
- GDPR Articles 6, 7, 13, 25 – Lawfulness, Consent, and Data Protection by Design

- ISO/IEC 27701 – Privacy Information Management System
- ViraShield Global Data Retention Schedule
- ViraShield Customer Consent Management Framework

4.2 Customer less Device Use Policy

Frameworks: NIST SP 800-53 (PT-2), GDPR Recital 26, ISO/IEC 27701

Policy #: VS-CDU-012

Policy Title: Customer less Device Use Policy

Policy Owner: Data Protection Officer (DPO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: External – Public & Regulatory

4.2.1 Purpose

The purpose of this policy is to formalize ViraShield’s commitment to user privacy by enabling product use without customer identity or login requirements. This approach supports privacy-by-design principles and ensures the company’s antivirus product can operate in environments where no user identity is provided or required.

4.2.2 Scope

This policy applies to:

- All ViraShield Portable AV devices sold globally.
- All customer interaction points that do not require account creation, email, or identity verification.
- All backend services handling device telemetry or subscription status where no user profile exist

4.2.3 Policy Statement

4.2.3.1 Customer less Operation Requirement

- Devices must be fully functional in their core security roles without requiring any identifiable customer data (PII).
- There shall be no requirement to:
  - Register for an account
  - Provide an email address or phone number
  - Submit personal identification for device activation

4.2.3.2 Subscription Enforcement Without Identity

- License validation will be based solely on anonymous device keys and secure tokens, without linking to end-user profiles.
- Subscription renewal notifications are delivered through:
  - Host screen prompts
  - Device LED indicators (where applicable)
  - Optional QR-based renewal links (non-tracking)

4.2.3.3 Anonymous Telemetry Handling

- When consent is granted, telemetry logs must:
  - Be stripped of any data that could reasonably identify the user or device owner
  - Use pseudonymized device IDs, randomized session tokens, and non-attributable scan results

4.2.3.4 Data Subject Exclusion Under GDPR

- As defined under GDPR Recital 26, customers who are not identifiable via the product's operation are not considered data subjects.
- Therefore, GDPR data subject rights (access, correction, erasure) are not applicable in default customer less usage unless consent is explicitly provided.

4.2.3.5 Regional Compliance Consideration

- Regions such as the EU, Singapore, and India require explicit documentation of data minimization practices.
- ViraShield must maintain internal records proving that devices function without PII collection, to satisfy regulatory inquiries.

4.2.4 Roles and responsibilities

- **Data Protection Officer (DPO) –** Reviews all product and telemetry designs to ensure compliance with customerless use principles.
- **Firmware Engineering Team** – Ensures no identity-requiring features are embedded in firmware unless toggled by user consent.
- **Cloud Licensing System Team** – Supports identity-free license validation logic and pseudonymized analytics handling.
- **Marketing & Support Teams** – May offer optional user registration features but must clearly state they are not required for use.

4.2.5 Enforcement

Any attempt to link device operation to a user's identity—without opt-in consent—violates this policy and may result in rollback of firmware features, internal investigation, and regional compliance violations. Regulatory fines and audit risk may apply in jurisdictions such as the EU or California.

4.2.6 Reference

- NIST SP 800-53 Rev. 5: PT-2 – Minimization of Personally Identifiable Information
- GDPR Recital 26 – Data Subject and Identifiability Principles
- ISO/IEC 27701 – Privacy Information Management System
- ViraShield Privacy & Consent Design Guidelines
- ViraShield Anonymous Subscription Management Framework
- ViraShield Global PII Minimization Report (Internal Only)

4.3 Customer Data Handling & Retention Policy

Frameworks: NIST SP 800-53 (SI-12), GDPR, ISO/IEC 27001:2022 (Annex A.8)

Policy #: VS-CDR-013

Policy Title: Customer Data Handling & Retention Policy

Policy Owner: Data Protection Officer (DPO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Restricted / Regulatory

4.3.1 Purpose

The policy governs how customer-related data is collected, stored, used, retained, and disposed of by ViraShield Technologies Inc. It ensures that all data handling practices are secure, legally compliant, purpose-specific, and respect user privacy, particularly for data processed through the ViraShield Portable AV platform and related cloud services.

4.3.2 Scope

This policy applies to:

- All customer-related data collected or processed by ViraShield, including:
  - Personal Identifiable Information (PII)
  - Device metadata
  - Licensing and subscription usage data
  - Consent audit logs

- All systems, personnel, and third parties who handle such data across global operations (USA, EU, APAC).

4.3.3 Policy Statement

4.3.3.1 Data Minimization & Purpose Limitation

- Devices Only data necessary for service delivery, support, security updates, and legal compliance may be collected.
- No excessive or non-essential PII (e.g., biometric data) may be collected without explicit justification and consent.

4.3.3.2 Secure Storage and Encryption

- All customer data must be:
  - Encrypted at rest and in transit (AES-256 and TLS 1.3 minimum)
  - Segmented by region based on data sovereignty (e.g., EU data processed in EU)
- Access must follow least privilege and be logged and monitored continuously

4.3.3.3 Data Retention Periods

- Customer PII and telemetry will be retained based on the following schedule:
  - Active subscription users: Up to 12 months after last use
  - Inactive/unsubscribed users: Deleted within 30 days of account expiry or consent withdrawal
  - Diagnostic logs: Retained up to 90 days unless consented otherwise
- All retention periods must be documented in the Data Retention Register and subject to biannual review.

4.3.3.4 Right to Access, Port, or Erase

- Per GDPR Articles 13 & 17, users have the right to:
  - Request access to their data (subject to verification)
  - Request full deletion (“right to be forgotten”) within 30 days of valid request
  - Receive data in a machine-readable format if requested

4.3.3.5 Vendor and Third-Party Handling

- Regions Vendors processing customer data must:
  - Be listed in the Vendor Risk Register
  - Sign a Data Processing Agreement (DPA) and agree to GDPR-equivalent safeguards
  - Use only approved and encrypted transport/storage mechanisms.

4.3.3.6 Data Disposal and Sanitization

- When retention periods expire or deletion requests are received:
  - Data must be wiped using NIST 800-88 compliant processes
  - Backups must be purged or overwritten within the deletion window
  - Logs of completed deletions must be maintained for 12 months

4.3.4 Roles and responsibilities

- **Data Protection Officer (DPO) –** Oversees all data handling procedures, audits, and compliance reporting
- **Legal & Compliance –** Verifies regulatory applicability and oversees DPA enforcement
- **DevOps & Cloud Security Teams –** Maintain encryption, backup purging, and data flow restrictions
- **Customer Support –** Processes access/erasure requests and responds to user inquiries on data rights

4.3.5 Enforcement

Violations of this policy, such as excessive retention or insecure storage of user data, may result in:

- Internal disciplinary action
- Third-party contract suspension
- Regulatory fines (e.g., GDPR penalties of up to 4% of global revenue)

4.3.6 Reference

- NIST SP 800-53 Rev. 5: SI-12 – Information Handling and Retention
- GDPR Articles 5, 13, 17 – Lawfulness and Rights of Erasure
- ISO/IEC 27001:2022 – Annex A.8: Secure Development
- ViraShield Data Retention Schedule
- ViraShield Vendor Risk Register
- ViraShield Consent and Deletion Request SOP

4.4 GDPR & CCPA Compliance Policy

Frameworks: NIST SP 800-53 (AR-8), GDPR, CCPA, ISO/IEC 27701

Policy #: VS-GCP-014

Policy Title: GDPR & CCPA Compliance Policy

Policy Owner: Data Protection Officer (DPO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: External – Regulatory

4.4.1 Purpose

The policy defines how ViraShield Technologies Inc. complies with the regulatory requirements of the General Data Protection Regulation (GDPR) for European Union data subjects and the California Consumer Privacy Act (CCPA) for California residents. It ensures transparency, legal processing, and consumer control over personal data within the scope of our hardware, licensing, and cloud-based threat intelligence systems.

4.4.2 Scope

This policy applies to:

- All personal data processed by ViraShield relating to EU or California users
- All customer interactions, telemetry processing, licensing services, and marketing communications
- Backend cloud infrastructure, analytics systems, customer support workflows, and vendor integrations that involve personal data

4.4.3 Policy Statement

4.4.3.1 Legal Basis for Processing

- For GDPR, personal data is processed based on:
  - Explicit user consent (Article 6.1a)
  - Contractual necessity (Article 6.1b)
  - Legitimate interests (Article 6.1f) with Data Protection Impact Assessment (DPIA)
- For CCPA, data collection is disclosed at the point of interaction, and no sale of personal information occurs without opt-out rights.

4.4.3.2 Privacy Notices and Consent

- ViraShield provides **clear and layered privacy notices** at or before the time of data collection.
- Notices must include:
  - Categories of data collected
  - Purpose of processing
  - User rights

- Contact details of the DPO

4.4.3.3 Consumer Rights Fulfillment

- ViraShield ensures:
  - Right to access and data portability (GDPR Art. 15, CCPA §1798.100)
  - Right to rectification and deletion (GDPR Art. 16–17, CCPA §1798.105)
  - Right to opt-out of data sharing or marketing
- All requests are honored within 30 calendar days, tracked in the internal Rights Request Register

4.4.3.4 Data Sharing and Third Parties

- Per All vendors with access to personal data:
  - Must sign a Data Processing Agreement (DPA)
  - Are listed publicly in the Privacy Notice
  - Must meet GDPR and CCPA-equivalent safeguards

4.4.3.5 Breach Notification

- Regions Any data breach involving EU or California user data must be:
  - Reported to authorities (e.g., supervisory authority under GDPR Article 33) within 72 hours
  - Notified to affected users when required by GDPR Article 34 or CCPA §1798.150

4.4.3.6 Data Minimization and Regional Compliance

- Only data necessary for service delivery is collected
- Data from EU and California is stored and processed in region, unless cross-border transfers are protected by:
  - SCCs (Standard Contractual Clauses)
  - Privacy frameworks (e.g., US-EU Data Privacy Framework)
  - Localized edge processing (if applicable)

4.4.4 Roles and responsibilities

- **Data Protection Officer (DPO)** – Owns this policy, leads regulatory response, and approves all public privacy notices
- **Legal & Compliance** – Verifies contracts, DPAs, and rights request workflows
- **IT & DevOps Teams** – Implement technical controls for data segregation, retention, and encryption

- **Marketing & Customer Success** – Ensure user-facing communications respect opt-out and consent boundaries

4.4.5 Enforcement

Any violation of this policy, including failure to uphold user rights, unauthorized data sharing, or delayed breach notifications, may result in regulatory penalties, internal disciplinary action, or termination of vendor relationships. Regulatory fines under GDPR or CCPA may be imposed based on severity, and repeated violations may trigger full compliance audits by internal or external authorities.

4.4.6 Reference

- NIST SP 800-53 Rev. 5: AR-8 – Privacy Notice and Consent
- GDPR: Articles 5, 6, 12–23, 33–34
- CCPA: California Civil Code §1798.100–1798.199
- ISO/IEC 27701 – Privacy Information Management System
- ViraShield Global Privacy Notice
- ViraShield Data Rights Management Procedure
- ViraShield Regulatory Breach Response SOP

5 Licensing & Subscription Policies

5.1 Product Activation & Subscription Policy

Frameworks: Internal Logic, PCI DSS

Policy #: VS-PAS-015

Policy Title: Product Activation & Subscription Policy

Policy Owner: Director of Licensing and Compliance

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Commercial / Licensing

5.1.1 Purpose

The purpose of this policy is to define the mechanisms and security controls governing product activation and subscription lifecycle management for the ViraShield Portable AV product line. The policy ensures subscription enforcement, compliance with payment data regulations, and a consistent customer experience without compromising security or privacy.

5.1.2 Scope

This policy applies to:

- All ViraShield-branded hardware products requiring activation or license validation
- Backend licensing infrastructure including secure license key storage and activation API endpoints
- Payment processors and subscription portals (Stripe, PayPal)
- Resellers and OEM partners distributing licensed versions of ViraShield products

5.1.3 Policy Statement

5.1.3.1 Product Activation Requirements

- All devices must be activated using a valid license key upon first use.
- Activation can occur through:
  - Direct USB connection to an internet-enabled device
  - QR code-based mobile activation
  - Offline activation mode using encrypted validation tokens

5.1.3.2 License Key Management

- TheLicense keys are:
  - Generated through a secure license provisioning system
  - Encrypted using RSA-2048 and stored in HSM-backed databases
  - Bound to unique device IDs using a cryptographic hash

5.1.3.3 Subscription Enforcement Logic

- Devices check license status via secure TLS 1.3 communication with ViraShield's cloud every 72 hours (if internet is available).
- If the subscription is expired or revoked:
- Core antivirus functions are downgraded to limited scan mode
- A warning is displayed on the host device or through companion app
- Subscription grace period: 14 days (after which features are locked)

5.1.3.4 Renewal and Upgrade Process

- Customers can renew via:
  - Auto-renewal linked to their chosen payment method
  - Manual key entry on device or mobile interface
  - Retail code redemption through partner portals

- Renewals are automatically reflected in the device's license state after validation

5.1.3.5 PCI DSS Compliance for Payment-Linked Activation

- All customer payment data is handled by third-party PCI-DSS certified processors.
- ViraShield does not store, process, or transmit cardholder data directly.
- Activation status is decoupled from payment credentials using transaction tokens.

5.1.3.6 Offline and Air-Gapped Use

- Offline devices:
  - Can operate using cached license data for up to 30 days
  - Must reconnect within the expiration window to remain functional
  - Air-gapped deployment options for regulated clients (e.g., government, healthcare) must be pre-approved and require signed SLA documentation

5.1.4 Roles and responsibilities

- **Director of Licensing and Compliance –** Owns this policy, oversees global license distribution, and ensures audit compliance
- **Cloud Licensing Engineering Team** – Maintains activation APIs, license databases, and renewal processing logic
- **Customer Support Team** – Assists users with activation errors, license resets, and offline scenarios
- **Finance & Payment Gateway Integrators** – Ensure PCI DSS adherence and manage payment renewals with certified vendors

5.1.5 Enforcement

Failure to comply with activation or subscription validation policies may result in restricted access to product functionality, loss of license entitlements, or termination of support. Unauthorized attempts to bypass activation or tamper with licensing mechanisms may lead to legal action and product deactivation.

5.1.6 Reference

- Internal Licensing Infrastructure Documentation
- PCI DSS v4.0 – Payment Security Standards
- ViraShield Secure Activation API Design Spec
- ViraShield Subscription Grace Period SOP

- ViraShield SLA Terms for Offline Clients

5.2 Payment Processing Policy

Frameworks: PCI DSS

Policy #: VS-PPP-016

Policy Title: Payment Processing Policy

Policy Owner: Chief Financial Officer (CFO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Financial / Regulatory

5.2.1 Purpose

This policy defines the procedures and security controls for processing customer payments securely and in compliance with the Payment Card Industry Data Security Standard (PCI DSS). It applies to all payment-related activities and systems associated with ViraShield’s subscription-based antivirus product and online storefront.

5.2.2 Scope

This policy applies to:

- All ViraShield payment systems and checkout flows (web, mobile, QR activation)
- Customer payment data transmitted through third-party processors
- Internal teams managing subscriptions, invoices, or refunds
- All vendors and partners handling any cardholder data on ViraShield’s behalf

5.2.3 Policy Statement

5.2.3.1 PCI DSS Compliance Requirements

- ViraShield must comply with PCI DSS v4.0 standards at all times.
- Only PCI DSS-certified processors (currently Stripe and PayPal) are authorized to process payment transactions.
- ViraShield systems do not store, process, or transmit full cardholder data.

5.2.3.2 Secure Payment Workflows

- All checkout pages must redirect users to secure hosted payment forms owned by PCI-compliant vendors.
- Card details are tokenized by vendors and used only to:
  - Initiate subscriptions
  - Process renewals

  - Issue refunds
  - hash

5.2.3.3 Payment Gateway Configuration

- APIs used to initiate or verify transactions must:
  - Use TLS 1.3 for encryption
  - Validate signatures and endpoint authentication
  - Be documented and tested quarterly for integrity

5.2.3.4 Audit and Logging

- All payment attempts (successful or failed) are logged with:
  - Token ID
  - Timestamp
  - Transaction result
  - Geographic metadata (country, IP)
- Logs are retained for 3 years to support PCI audit requirements

5.2.3.5 Customer Notification & Consent

- All billing events (charges, renewals, failures) must trigger email notifications to customers.
- Subscription terms and cancellation policies must be disclosed before payment is submitted.
- Refund policies must be available via the customer dashboard and support portal.

5.2.3.6 Payment Dispute Handling

- Disputes (chargebacks, refunds, etc.) must be processed within 10 business days.
- All cases are logged, assigned a reference ID, and escalated to the finance team when needed.

5.2.4 Roles and responsibilities

- **Chief Financial Officer (CFO) –** Owns this policy and oversees financial compliance with PCI DSS
- **Finance & Billing Department –** Manages day-to-day transactions, reconciliations, and dispute resolution
- **Payment Gateway Integrators –** Maintain API tokens, gateway configs, and ensure TLS validation

- **Customer Success & Support –** Assists customers with failed transactions, billing errors, or cancellations

5.2.5 Enforcement

Any employee or vendor who bypasses authorized payment workflows, stores unencrypted cardholder data, or uses unauthorized gateways will face immediate investigation. Breaches of this policy may lead to financial penalties, regulatory audits, vendor termination, or legal action.

5.2.6 Reference

- PCI DSS v4.0 Standard
- Stripe PCI DSS Compliance Documentation
- PayPal Secure Payments Integration Guide
- ViraShield Finance Team Internal Billing SOP
- ViraShield Customer Refund and Dispute Policy

5.3 License Key Verification & Renewal Policy

Frameworks: NIST SP 800-53 (CM-5), ISO/IEC 27001:2022 (Annex A.9)

Policy #: VS-LKR-017

Policy Title: License Key Verification & Renewal Policy

Policy Owner: Director of Licensing and Compliance

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Licensing & Security

5.3.1 Purpose

This purpose of this policy is to define the controls, processes, and responsibilities governing the secure verification, renewal, and revocation of license keys associated with ViraShield's Portable AV products. It ensures license enforcement, security of device authentication, and compliance with access control frameworks.

5.3.2 Scope

This policy applies to:

- All issued ViraShield license keys (standard, trial, corporate, or OEM)
- Backend cloud infrastructure responsible for key validation and renewal
- Firmware modules validating license locally or via secure OTA

- All teams managing license generation, validation, enforcement, or audit

5.3.3 Policy Statement

5.3.3.1 License Key Structure and Security

- License keys must:
  - Be cryptographically signed using RSA 2048 or ECC keys
  - Contain device binding data (e.g., unique device hash, product version)
  - Be unreadable in plaintext from the device memory or firmware

5.3.3.2 Verification Process

- On every internet connection (max interval: 72 hours), devices must:
  - Validate license status through a secure TLS 1.3 connection
  - Check expiration date, subscription type, and signature validity
  - Flag revoked, expired, or tampered licenses and downgrade functionality
- Offline license verification (fallback):
  - Permitted for up to 30 days using locally cached encrypted key metadata

5.3.3.3 Renewal Triggers

- Automatic renewal is triggered via:
  - Linked payment account (auto-renew customers)
  - Manual redemption of activation codes (retail/OEM clients)
  - Admin-controlled re-keying process (for enterprise/healthcare clients)
- Devices must reflect updated license status within 6 hours of successful renewal

5.3.3.4 Key Revocation & Tampering Detection

- Revoked keys (e.g., due to fraud or misuse) are added to the real-time revocation list (RRL)
- Devices checking into the license server are compared against RRL
- If tampering is detected:
  - Device access is restricted
  - Logs are uploaded for forensic analysis
  - Firmware revalidation is enforced on next boot

5.3.3.5 Logging & Monitoring

- All license key checks must be logged with:
  - Device hash
  - License type and expiry date

  - Timestamp of last sync
  - Status of verification (valid, expired, revoked, mismatched)
- Logs are retained for a minimum of 24 months to support licensing audits

5.3.4 Roles and responsibilities

- **Director of Licensing and Compliance** – Owns the policy, signs off license architecture, and oversees audit compliance
- **Cloud Licensing Team** – Implements verification endpoints, revocation logic, and telemetry collection
- **Firmware Engineering Team** – Integrates secure key handling into embedded systems
- **Support Team** – Handles renewal failures, revoked licenses, and offline activation cases

5.3.5 Enforcement

Unauthorized access attempts using expired or tampered keys may result in immediate service restriction, forensic review, and permanent device deactivation. Employees or vendors responsible for failed renewals or insecure key handling may be subject to internal investigation or termination.

5.3.6 Reference

- NIST SP 800-53 Rev. 5: CM-5 – Access Restrictions for Change
- ISO/IEC 27001:2022 – Annex A.9: Access Control
- ViraShield License Integrity Verification Framework
- ViraShield License Revocation & Tampering Response SOP
- ViraShield License Expiry Notification Standards

5.4 Account Termination and Data Deletion Policy

Frameworks: NIST SP 800-53 (MP-6), GDPR, CCPA

Policy #: VS-ADD-018

Policy Title: Account Termination and Data Deletion Policy

Policy Owner: Data Protection Officer (DPO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: External – Regulatory / User Rights

5.4.1 Purpose

This policy defines the procedures and responsibilities for securely terminating user accounts and deleting associated data upon request or inactivity, in compliance with international data privacy and protection regulations. It ensures ViraShield respects user rights to deletion while maintaining audit integrity and minimizing residual data risk.

5.4.2 Scope

This policy applies to:

- All user accounts, subscription records, and associated PII processed by ViraShield
- Data subject to deletion requests under GDPR and CCPA
- Customer data stored in databases, backup systems, cloud services, device activation logs, and telemetry repositories

5.4.3 Policy Statement

5.4.3.1 User-Initiated Account Termination

- Users may terminate accounts via:
  - The customer dashboard (self-service)
  - A written/email request to the Data Protection Officer
- Upon account termination:
  - Subscription is immediately canceled
  - Associated device licenses are invalidated or decoupled
  - A final data deletion confirmation email is sent

5.4.3.2 Data Deletion Request Handling

- Per GDPR Article 17 and CCPA §1798.105, users may request:
  - Full deletion of their account and associated data
  - Partial deletion (e.g., PII only, retaining device logs anonymously)
- All requests must be verified through identity validation and processed within 30 calendar days

5.4.3.3 Data Sanitization Standards

- Data must be securely deleted using one or more of the following:
  - Cryptographic erasure for cloud databases
  - Secure overwrite techniques for on-premises media (per NIST 800-88)
  - Token/pseudonym unlinking in analytics systems

- Backups containing user data must be excluded from future recovery cycles within 30 days

5.4.3.4 Inactive Account Purge

- Revoked keys (e.g., due to fraud or misuse) are added to the real-time revocation list (RRL)
- Devices checking into the license server are compared against RRL
- If tampering is detected:
  - Device access is restricted
  - Logs are uploaded for forensic analysis
  - Firmware revalidation is enforced on next boot

5.4.3.5 Logging & Monitoring

- Inactive accounts (12 months of inactivity) are flagged for deletion
- Users are notified 30 days in advance with an option to retain or export data
- If no response, accounts are auto deleted, and deletion logs are retained internally

5.4.3.6 Data Retention Exceptions

- Certain data may be retained if required by:
- Legal/regulatory obligations (e.g., tax compliance, security audits)
- Active legal investigations (with data freeze applied)
- Service provisioning where the user has opted into extended retention

5.4.4 Roles and responsibilities

- **Data Protection Officer (DPO)** – Reviews and approves deletion processes, handles legal/regulatory queries
- **IT Operations Team** – Executes deletion in production and backup systems, ensures wipe logging
- **Customer Support** – Assists users in termination requests and identity verification
- **Legal & Compliance** – Validates whether any exemptions or freezes apply to deletion requests

5.4.5 Enforcement

Improper retention, delayed deletion, or unauthorized reactivation of terminated accounts may result in disciplinary action, audit review, or fines under GDPR or CCPA. Any employee or vendor failing to comply with this policy may be subject to internal investigation or contract penalties.

5.4.6 Reference

- NIST SP 800-53 Rev. 5: MP-6 – Media Sanitization
- GDPR Article 17: Right to Erasure
- CCPA §1798.105: Consumer Right to Delete
- ViraShield Data Retention & Purge Schedule
- ViraShield User Rights Request SOP
- ViraShield Cryptographic Erasure Implementation Guide

6 Cloud Infrastructure Policies

6.1 Cloud Security Policy

Frameworks: NIST SP 800-53 (SC-12), ISO/IEC 27017

Policy #: VS-CSP-019

Policy Title: Cloud Security Policy

Policy Owner: Cloud Infrastructure Security Manager

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Infrastructure Security

6.1.1 Purpose

The purpose of this policy is to define the security standards for managing and protecting ViraShield's cloud-based infrastructure, services, and customer data. This includes ensuring secure provisioning, monitoring, and lifecycle management of cloud systems that support licensing validation, OTA updates, threat telemetry, and user consent logs.

6.1.2 Scope

This policy applies to:

- All cloud-hosted infrastructure and services operated by or for ViraShield Technologies
- Public, private, and hybrid cloud environments (e.g., AWS, Azure)
- Cloud services supporting production, licensing, and global telemetry functions
- All personnel with administrative or development access to cloud systems

6.1.3 Policy Statement

6.1.3.1 Secure Cloud Architecture

- All cloud infrastructure must be deployed using:
  - Role-based access control (RBAC)
  - Virtual private clouds (VPCs) with restricted ingress/egress
  - Multi-tier architecture separating frontend, backend, and telemetry services

6.1.3.2 Identity and Access Controls

- All cloud access must:
  - Be integrated with MFA-enabled identity providers
  - Be audited and reviewed quarterly for privilege escalation
  - Restrict admin roles to cloud security engineers only
- Access provisioning must follow a least-privilege and time-bound principle

6.1.3.3 Infrastructure-as-Code (IaC) Security

- All cloud deployments must use version-controlled IaC templates (e.g., Terraform, CloudFormation)
- IaC templates must be scanned for misconfigurations and secrets prior to deployment using automated tools

6.1.3.4 Monitoring, Logging, and Alerting

- All cloud activities must be:
  - Logged in real-time via native tools (e.g., AWS CloudTrail, Azure Monitor)
  - Stored for at least 12 months in immutable log storage
  - Integrated with SIEM for anomaly detection and incident response

6.1.3.5 Vendor and Cloud Service Provider Compliance

- All cloud providers must:
  - Be ISO/IEC 27017 and 27001 certified
  - Support data residency in user-defined geographies
  - Sign a Cloud Data Processing Agreement (CDPA)

6.1.4 Roles and responsibilities

- **Cloud Infrastructure Security Manager** – Oversees cloud configuration, monitoring, and compliance
- **DevOps and Cloud Engineers** – Implement secure provisioning and maintain IaC pipelines
- **Security Operations Center (SOC)** – Monitors cloud activity and responds to alerts

- **Compliance and Legal Teams** – Ensure that cloud providers meet regulatory and contractual obligations

6.1.5 Enforcement

Misuse of cloud access credentials, misconfigured infrastructure, or failure to apply security updates may result in revocation of access, performance reviews, or termination. Security incidents traced to cloud negligence will trigger forensic review and potential escalation to executive oversight.

6.1.6 Reference

- NIST SP 800-53 Rev. 5: SC-12 – Cryptographic Key Establishment
- ISO/IEC 27017: Code of Practice for Cloud Information Security
- ViraShield Cloud Security Architecture Diagram
- ViraShield Key Management and Access Matrix
- AWS Well-Architected Security Pillar
- Azure Security Benchmark v3

6.2 Encryption and Key Management Policy

Frameworks: NIST SP 800-53 (SC-12, SC-13), ISO/IEC 27001:2022 (Annex A.10)

Policy #: VS-EKM-020

Policy Title: Encryption and Key Management Policy

Policy Owner: Chief Information Security Officer (CISO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Cryptographic Security

6.2.1 Purpose

The purpose of this policy is to define the standards for the secure use of cryptographic algorithms and the protection of cryptographic keys across all environments at ViraShield Technologies Inc. This includes encryption of data in transit and at rest, key generation, storage, rotation, and disposal — especially in cloud, firmware, and device communication.

6.2.2 Scope

This policy applies to:

- All systems, databases, cloud services, and firmware using cryptographic operations

- All cryptographic keys used for encryption, authentication, licensing, and firmware validation
- All personnel managing or interacting with cryptographic key infrastructure (CKI), including cloud-based key vaults and hardware security modules (HSMs)

6.2.3 Policy Statement

6.2.3.1 Encryption Standards

- At rest:
  - All sensitive data must be encrypted using AES-256 or stronger
  - Device logs, telemetry, customer PII, and license metadata must be encrypted on storage volumes or firmware flash
- In transit:
  - All internal and external communications must use TLS 1.3 or higher
  - Public APIs must enforce HTTPS using valid, up-to-date certificates

6.2.3.2 Key Generation and Storage

- All cryptographic keys must be:
  - Generated using FIPS 140-2 validated libraries
  - Stored securely in HSMs or cloud-native key vaults (e.g., AWS KMS, Azure Key Vault)
  - Accessible only by authorized services and personnel based on role

6.2.3.3 Key Access and Segregation

- Key access controls must:
  - Follow the principle of least privilege
  - Be audited monthly to detect over-permissioning or unauthorized access
  - Be segregated by environment (dev, test, production) and function (signing, encryption, licensing)

6.2.3.4 Key Rotation and Expiry

- All production keys must be:
  - Rotated at least every 12 months (or upon compromise/event trigger)
  - Versioned with backward compatibility and rollback capability
  - Firmware signing keys must follow quarterly rotation cycles with audit trails

6.2.3.5 Key Revocation and Destruction

- If a key is suspected of compromise:
  - It must be revoked immediately from the key store

  - All dependent systems must be rekeyed or fallback to fail-safe logic
- Expired or unused keys must be cryptographically erased using NIST 800-88 secure destruction standards

6.2.3.6 Monitoring and Audit

- All key-related events (creation, access, rotation, deletion) must be logged
- Logs must be:
  - Retained for a minimum of 24 months
  - Reviewed quarterly by the Information Security team
  - Integrated with centralized SIEM for anomaly detection

6.2.4 Roles and responsibilities

- **Chief Information Security Officer (CISO)** – Owns and approves this policy, ensures compliance with frameworks
- **Cloud Infrastructure Team** – Implements encryption protocols and manages key vault access in production
- **Firmware Team** – Ensures cryptographic integrity of signed firmware and device-level encryption
- **IT Security Operations** – Monitors key use, revocation events, and performs key-related audits

6.2.5 Enforcement

Any unauthorized use, exposure, or mismanagement of cryptographic keys may result in immediate revocation of system access, full audit of affected infrastructure, and disciplinary or legal action. Compliance failures tied to encryption can lead to regulatory investigation under GDPR, PCI DSS, or NIST-aligned audits.

6.2.6 Reference

- **NIST SP 800-53 Rev. 5**: SC-12 – Cryptographic Key Establishment, SC-13 – Cryptographic Protection
- **ISO/IEC 27001:2022 – Annex A.10**: Cryptographic Controls
- ViraShield Encryption Protocol Implementation SOP
- ViraShield Key Management Lifecycle Plan
- AWS Key Management Best Practices
- Azure Key Vault Security and Compliance Whitepaper

6.3 Logging and Monitoring Policy

Frameworks: NIST SP 800-53 (AU-2 to AU-12), ISO/IEC 27001:2022 (Annex A.12)

Policy #: VS-LMP-021

Policy Title: Logging and Monitoring Policy

Policy Owner: Information Security Operations Manager

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Operational Security

6.3.1 Purpose

The purpose of this policy is to establish consistent and secure practices for system logging, monitoring, and audit log management across all infrastructure components. This supports threat detection, forensic readiness, regulatory compliance, and the overall integrity of ViraShield's security operations.

6.3.2 Scope

This policy applies to:

- All cloud systems, on-prem infrastructure, firmware, and endpoint security systems
- Security Information and Event Management (SIEM) tools used by ViraShield
- Internal systems such as identity platforms, licensing servers, AV telemetry, and OTA update services
- Employees and third-party providers managing or accessing audit logs

6.3.3 Policy Statement

6.3.3.1 Logging Requirements

- All systems must log:
  - Authentication events (login/logout, MFA use)
  - Privileged user activity
  - License key checks and OTA update attempts
  - AV threat detections and telemetry uploads
  - Configuration changes and firmware deployments
- Logs must include:
  - Timestamp (in UTC)
  - User ID or system ID
  - Source IP address

  - Event type and outcome
  - Device ID (if applicable)
  - -to-date certificates

6.3.3.2 Log Storage and Retention

- All logs must be:
  - Transmitted securely to a centralized SIEM platform (e.g., Splunk, Azure Sentinel)
  - Stored in immutable format for a minimum of 24 months
  - Segregated by environment (prod/dev/test) and sensitivity
- Backup copies must be encrypted and stored offsite or in redundant cloud zones

6.3.3.3 Monitoring and Alerting

- Real-time monitoring must be in place for:
  - Authentication anomalies (e.g., failed logins, geolocation mismatch)
  - Elevated privilege activity
  - Suspicious USB or firmware behavior
  - System integrity failures
- SIEM must be configured to:
  - Generate alerts for critical security events
  - Escalate alerts to the Security Operations Center (SOC) within 15 minutes
  - Trigger incident response playbooks when thresholds are exceeded

6.3.3.4 Access to Audit Logs

- Access to audit logs must be:
  - Limited to authorized personnel only (SOC, CISO, auditors)
  - Granted via role-based access control (RBAC)
  - Logged and reviewed quarterly for anomalies

6.3.3.5 Forensic Readiness

- Logs must be:
  - Structured to support legal admissibility and digital forensics
  - Time-synchronized via NTP to maintain timestamp accuracy
  - Retained in accordance with any legal hold or data breach investigation requirements

6.3.4 Roles and responsibilities

- **Information Security Operations Manager** – Oversees SIEM configurations, log integrity, and policy enforcement
- **Security Operations Center (SOC)** – Monitors log data, investigates anomalies, and escalates confirmed threats
- **IT Infrastructure Team** – Ensures that systems are logging as per configuration baselines
- **Compliance and Audit Team** – Reviews logs during quarterly security audits and regulatory checks

6.3.5 Enforcement

Failure to configure proper logging or respond to monitoring alerts in a timely manner may result in disciplinary action, revocation of access privileges, or audit remediation requirements. Deliberate log tampering or suppression of alerts will result in immediate escalation to the CISO and Legal team.

6.3.6 Reference

- NIST SP 800-53 Rev. 5: AU-2 to AU-12 – Audit and Accountability Controls
- ISO/IEC 27001:2022 – Annex A.12: Logging and Monitoring
- ViraShield SIEM Configuration Guide
- ViraShield Log Retention and Backup SOP
- Azure Monitor & AWS CloudTrail Integration Standards
- ViraShield Forensic Log Preservation Checklist

6.4 Network Segmentation & Firewall Policy

Frameworks: NIST SP 800-53 (SC-7), CIS Controls v8

Policy #: VS-NSF-022

Policy Title: Network Segmentation & Firewall Policy

Policy Owner: Network Security Architect

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Network Security

6.4.1 Purpose

The purpose of this policy is to define network segmentation, firewall configuration, and boundary protection requirements across all environments at ViraShield Technologies Inc. It ensures secure isolation of critical systems, reduces the attack surface, and prevents unauthorized lateral movement within networked environments.

6.4.2 Scope

This policy applies to:

- All physical and virtual networks at ViraShield (on-premise, cloud, hybrid)
- Public cloud environments (AWS, Azure) supporting licensing, OTA, and telemetry infrastructure
- Internal VLANs, micro-segmentation policies, and firewall appliances
- All IT, DevOps, and Engineering personnel managing network-connected assets

6.4.3 Policy Statement

6.4.3.1 Segmentation Architecture

- ViraShield networks must be logically segmented into security zones:
- Public Zone – API gateways, website frontends, telemetry submission interfaces
- DMZ – Load balancers, proxy servers, license sync services
- Protected Internal Zone – Application servers, cloud databases, OTA backend
- Restricted Zone – Source code repositories, admin consoles, signing servers
- No direct traffic may traverse zones without passing through a stateful inspection point (e.g., firewall, WAF)

6.4.3.2 Firewall Standards

- All perimeter and internal firewalls must:
  - Deny-all by default and allow-by-exception
  - Be configured with documented rule sets aligned to least privilege
  - Support deep packet inspection (DPI) and application-layer filtering
  - Log all dropped or suspicious traffic

6.4.3.3 Micro-Segmentation

- In cloud environments:
  - Use native controls (e.g., AWS Security Groups, Azure NSGs) to enforce VM-level isolation

  - Tag and group workloads by environment (dev/test/prod), sensitivity, and owner
  - Limit East-West traffic across VMs and containers

6.4.3.4 Change Control and Rule Reviews

- Firewall rules must be:
  - Requested via change management tickets
  - Reviewed and approved by the Network Security Architect
  - Audited quarterly for redundancy, expired exceptions, and risk exposure

6.4.3.5 Monitoring and Response

- All firewall and IDS/IPS systems must:
  - Forward logs to the central SIEM within 60 seconds of generation
  - Trigger alerts for port scans, DDoS attempts, or unauthorized internal probing
  - Be tested every 6 months for failover and rule enforcement accuracy.

6.4.3.6 Remote Access Boundaries

- All VPN or remote access connections must:
- Terminate in a hardened DMZ segment
- Pass through a gateway firewall before reaching internal systems
- Be subject to geo-restrictions and time-of-day controls for privileged accounts

6.4.4 Roles and responsibilities

- **Network Security Architect** – Designs segmentation architecture, approves rule changes, oversees firewall audits
- **Infrastructure and DevOps Teams** – Implement zone assignments, maintain firewall rule documentation
- **SOC Analysts** – Monitor logs and investigate alerts generated by firewalls and segmentation breaches
- **Compliance Team** – Validates network security controls during internal and external audits

6.4.5 Enforcement

Improper segmentation, misconfigured firewall rules, or unauthorized access between network zones may result in a formal security review, remediation mandates, or access revocation. Repeated noncompliance will be escalated to the CISO and may result in termination or contract suspension.

6.4.6 Reference

- NIST SP 800-53 Rev. 5: SC-7 – Boundary Protection
- CIS Controls v8: Safeguards 4, 11, and 13 – Network Segmentation and Access Control
- ViraShield Network Topology Diagram
- ViraShield Firewall Rule Change SOP
- AWS VPC and Security Group Hardening Guide
- Azure Virtual Network Segmentation and NSG Best Practices

7 Incident Response & Continuity Policies

7.1 Incident Response Policy

Frameworks: NIST SP 800- 61, ISO/IEC 27001:2022 (Annex A.16)

Policy #: VS-IRP-023

Policy Title: Incident Response Policy

Policy Owner: Chief Information Security Officer (CISO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Security Operations

7.1.1 Purpose

This policy defines the procedures and responsibilities for detecting, reporting, assessing, responding to, and recovering from information security incidents at ViraShield Technologies Inc. The goal is to minimize damage, reduce recovery time, ensure regulatory compliance, and continuously improve defensive capabilities.

7.1.2 Scope

This policy applies to:

- All ViraShield IT systems, cloud services, firmware platforms, and AV devices
- Employees, contractors, and third-party service providers handling company infrastructure or data
- All incidents involving unauthorized access, data breaches, malware detection, service interruption, or suspected compromise of critical systems

7.1.3 Policy Statement

7.1.3.1 Incident Definition and Classification

- All incidents will be categorized by severity and type:
  - Level 1 – Critical: Data breach, ransomware, cloud compromise
  - Level 2 – High: Unauthorized access, malware detection on endpoint or USB AV device
  - Level 3 – Medium/Low: Policy violations, phishing attempts, failed login escalations

7.1.3.2 Reporting Requirements

- Incidents must be reported within **30 minutes** of discovery to the SOC or CISO
- Security event reports should include:
  - Timestamp and detection method
  - System(s) affected
  - Description and suspected impact
- Anonymous reporting is allowed via the internal hotline or portal

7.1.3.3 Response Lifecycle

- The Incident Response Team (IRT) must follow this standardized lifecycle:

1. **Preparation** – Develop and maintain IR tools, communication plans, and training
2. **Identification** – Analyze events and confirm whether they constitute an incident
3. **Containment** – Isolate affected systems to prevent further damage
4. **Eradication** – Remove root cause artifacts (e.g., malware, access vectors)
5. **Recovery** – Restore services and verify systems are clean and patched
6. **Lessons Learned** – Conduct a post-incident review and update procedures

7.1.3.4 Response Team Activation

- The **Incident Response Team (IRT)** will include:
  - CISO (Lead)
  - IT Security Manager
  - Legal Counsel (if regulatory reporting required)
  - Communications Lead
- IRT roles and contact methods must be documented and reviewed quarterly

7.1.3.5 Digital Forensics and Evidence Handling

- Preserve volatile memory, logs, and system snapshots where applicable
- Chain of custody forms must be maintained if evidence is to be used legally

- External forensic specialists may be engaged for major incidents

7.1.3.6 Regulatory Notification

- The DPO and Legal Counsel will coordinate notifications for:
  - GDPR: within 72 hours of breach awareness
  - CCPA, HIPAA, PCI DSS: according to local/regulatory timelines
  - Customers, partners, or insurers as required by contract

7.1.3.7 Testing and Continuous Improvement

- IR plans must be tested semi-annually via tabletop or live exercises
- All incidents will be followed by:
  - A formal post-incident review
  - Updated risk assessments and policy refinement
  - Team retraining if gaps are identified

7.1.4 Roles and responsibilities

- **Chief Information Security Officer (CISO)** – Owns incident response program, approves reports, oversees lifecycle activities
- **Security Operations Center (SOC) –** Detects and triages incidents 24/7, escalates critical events
- **Incident Response Team (IRT)** – Executes containment, investigation, and recovery tasks
- **Legal & Compliance** – Determines disclosure obligations, interacts with regulatory bodies
- **All Users** – Required to report suspicious activity without delay

7.1.5 Enforcement

Deliberate suppression of incident reports, failure to cooperate with investigations, or mishandling of sensitive evidence may result in disciplinary actions, up to and including termination. Failure to meet regulatory notification deadlines may result in financial and legal liability for the organization.

7.1.6 Reference

- NIST SP 800- 61 Rev. 2: Computer Security Incident Handling Guide
- ISO/IEC 27001:2022 – Annex A.16: Incident Management
- ViraShield Incident Response Playbook
- ViraShield SIEM Alert Triage SOP
- GDPR Article 33, CCPA §1798.82 – Breach Notification

- ViraShield Chain of Custody Form

7.2 Backup & Disaster Recovery Policy

Frameworks: NIST SP 800-53 ((CP-9), ISO/IEC 27001:2022 (Annex A.17)

Policy #: VS-BDRP-024

Policy Title: Backup & Disaster Recovery Policy

Policy Owner: Chief Technology Officer (CTO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Business Continuity

7.2.1 Purpose

To ensure the ongoing availability, integrity, and recoverability of data and critical business systems at ViraShield Technologies Inc. This policy establishes responsibilities and procedures for performing data backups and implementing disaster recovery strategies across infrastructure and product-related services.

7.2.2 Scope

This policy applies to:

- Cloud infrastructure (AWS, Azure) supporting licensing, OTA updates, and telemetry
- Internal documentation, firmware source code, and product configurations
- Critical business systems including customer portals, licensing servers, and security log storage
- All personnel responsible for maintaining IT operations, cloud environments, and product update distribution

7.2.3 Policy Statement

7.2.3.1 Data Backup Requirements

- Full system and database backups must occur daily for production systems and weekly for development environments
- Backup copies must be encrypted at rest and during transmission using AES-256 and TLS 1.3
- Backups must be stored in geographically separate cloud regions (e.g., AWS U.S. East and EU Central)
- Backups will include:

  - License key database
  - OTA firmware update metadata
  - Telemetry logs and AV detection data (anonymized)
  - Source code repositories and internal documentation

7.2.3.2 Backup Testing and Validation

- All Restore testing must be conducted quarterly on a randomized subset of backup archives
- Testing must verify:
  - Integrity and completeness of restored files
  - Functionality of core systems after restoration
  - Minimal data loss tolerance within Recovery Point Objective (RPO) of 24 hours

7.2.3.3 Disaster Recovery Planning

- A full Disaster Recovery Plan (DRP) shall be maintained and reviewed annually
- It must address:
  - Cloud environment re-deployment
  - Incident-specific continuity for product updates and license validation
  - Communications plan for stakeholders and customers
  - Roles, failover timelines, and contact information

7.2.3.4 Recovery Objectives

- Recovery Time Objective (RTO): Critical production services (e.g., license validation, OTA) must be restored within 4 hours of outage detection
- Recovery Point Objective (RPO): Data loss must not exceed 24 hours for customer or operational systems
- All systems must log restoration completion, tested functionality, and verification timestamps

7.2.3.5 Product Backup Procedures

- Firmware release branches and trained AI malware models must be stored in:
  - Secure offline archives quarterly
  - Immutable S3 buckets with versioning
  - Endpoint devices must be able to resume OTA services upon license validation via redundant DNS endpoints

7.2.3.6 Third-Party Dependencies

- Firmware Backup vendors must provide:
  - SOC 2 Type II certification or equivalent
  - Encryption-at-rest guarantees
  - DR testing reports available upon request

7.2.4 Roles and responsibilities

- **Chief Technology Officer (CTO):** Owns BDR strategy, approves recovery plan and backup architecture
- **Infrastructure Team:** Performs backups, manages restore testing, validates encryption
- **Cloud Services Manager:** Coordinates cloud failover and region-based replication
- **Compliance Officer:** Ensures recovery controls align with legal and regulatory expectations
- **Development Team:** Verifies integrity of source code and OTA update artifacts post-restoration

7.2.5 Enforcement

Failure to follow defined backup or DR protocols, or mismanagement of backup encryption, may result in immediate audit and escalation to the CISO or CTO. Intentional neglect may lead to disciplinary action including revocation of administrative privileges or termination.

7.2.6 Reference

- NIST SP 800-53 Rev. 5 (CP-9): Contingency Planning – Information System Backup
- ISO/IEC 27001:2022 – Annex A.17: Information Security Aspects of Business Continuity
- ViraShield Disaster Recovery Plan
- AWS Backup and Cross-Region Replication SOP
- ViraShield Cloud Encryption Standards
- SOC 2 Type II Audit Framework (3rd party vendor compliance)

7.3 Breach Notification Policy

Frameworks: NIST SP 800-53 (IR-6), GDPR, HIPAA

Policy #: VS-BNP-025

Policy Title: Breach Notification Policy

Policy Owner: Chief Information Security Officer (CISO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Legal & Regulatory

7.3.1 Purpose

To establish a consistent process for the identification, assessment, and timely reporting of data breaches that affect the confidentiality, integrity, or availability of sensitive data handled by ViraShield Technologies Inc. This policy ensures compliance with global regulatory obligations and protection of customer trust.

7.3.2 Scope

This policy applies to:

- All employees, contractors, and third-party vendors
- All systems handling personal data, health-related information, payment data, and customer telemetry
- All incidents that may involve unauthorized disclosure or access to regulated data including PII, PHI, PCI, or IP assets

7.3.3 Policy Statement

7.3.3.1 Encryption Standards

- Any suspected breach must be reported immediately to the SOC for triage
- The CISO and Legal Counsel will assess:

○ Whether a breach occurred under GDPR Article 4, HIPAA §164.402, or other applicable laws

○ Type and volume of data affected

○ Potential impact on data subjects, customers, or partners

7.3.3.2 Key Generation and Storage

- ViraShield is committed to notifying affected parties and regulators within required timelines:

○ GDPR: Supervisory authority within 72 hours of breach awareness

○ HIPAA: Notification to HHS and affected individuals within 60 days

○ PCI DSS/contractual partners: Within 5 business days or as defined by SLAs

7.3.3.3 Notification Content

- Notifications must include:

○ A clear description of the incident and breach type

  - Categories and volume of data affected
  - Mitigation steps taken
  - Recommendations for affected individuals
  - Contact information for follow-up and rights requests

7.3.3.4 Communication Channels

- Regulator notifications will be submitted via official portals (e.g., GDPR Data Protection Authority portal, HHS portal)
- Affected individuals will be notified via email or public statements depending on scale
- Notification templates must be pre-approved by the Legal and Compliance departments

7.3.3.5 Documentation and Audit Trail

- Every breach must have a full incident report logged in the IR system
- Documentation must include evidence of:
  - Detection timeline
  - Escalation steps
  - Notification approvals
  - Final actions taken and mitigation

7.3.3.6 Exceptions and Delays

- Delayed notifications may only occur if:
  - Directed by law enforcement
  - Additional forensics are required to validate breach scope
  - Legal review justifies limited disclosure initially
- Such exceptions must be approved and documented by the CISO and General Counsel

7.3.4 Roles and responsibilities

- **Chief Information Security Officer (CISO):** Oversees breach impact analysis and coordinates technical aspects
- **Legal Counsel:** Determines legal obligations and reviews outbound communications
- **Compliance Officer:** Maintains awareness of applicable breach laws per region
- **IT Security & SOC Team:** Provides breach details, logs, and technical indicators
- **Public Relations Lead:** Coordinates external messaging if mass disclosure is required

7.3.5 Enforcement

Failure to report a breach or delay notification may result in legal liability, regulatory fines, and disciplinary action including termination. All staff are obligated to report suspected security incidents without delay.

7.3.6 Reference

- NIST SP 800-53 Rev. 5 (IR-6): Incident Reporting
- GDPR Articles 33 and 34
- HIPAA Breach Notification Rule (45 CFR §§164.400–414)
- ViraShield Incident Reporting SOP
- ViraShield Regulatory Notification Template
- ISO/IEC 27701 Privacy Controls (supporting guideline)

7.4 Business Continuity Plan (BCP)

Frameworks: NIST SP 800-53 (CP-2), ISO 22301

Policy #: VS-BCP-026

Policy Title: Business Continuity Plan (BCP)

Policy Owner: Chief Operating Officer (COO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Continuity & Risk Management

7.4.1 Purpose

To establish a business continuity strategy that enables ViraShield Technologies Inc. to maintain essential operations during and after disruptive events. This policy defines the planning, governance, and procedures needed to ensure continuity of service, customer trust, and compliance during cyber incidents, natural disasters, infrastructure failures, and pandemics.

7.4.2 Scope

This policy applies to:

- All departments and business-critical functions across global offices
- Infrastructure supporting licensing servers, OTA update systems, subscription validation, and cloud-hosted firmware distribution
- All product-facing operations including support, AV intelligence processing, and device license integrity systems

- Offices in Austin (HQ), Bangalore, Frankfurt, and Singapore

7.4.3 Policy Statement

7.4.3.1 Continuity Planning Requirements

- A formal BCP must be developed and maintained by the COO's office in collaboration with department heads
- Plans must cover:
  - Threat scenarios (e.g., DDoS, data center outages, supply chain failure, pandemic disruptions)
  - Communication hierarchy and failover lines
  - Alternate sites and work-from-anywhere strategies
  - Prioritized Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)

7.4.3.2 Business Impact Analysis (BIA)

- A BIA must be conducted annually to:
  - Identify critical assets, personnel, and suppliers
  - Quantify financial and operational impact of downtime
  - Prioritize restoration order of key services (e.g., license auth, product firmware portal)
  - Determine dependencies across physical and cloud assets

7.4.3.3 Plan Testing and Maintenance

- BCP must be tested biannually using tabletop simulations and real-time recovery drills
- Test results must be documented and used to revise and optimize procedures
- All key personnel must receive BCP training and incident role assignments

7.4.3.4 Communication and Escalation

- Emergency communication protocols will be managed by the COO and Communications Team
- Internal and external updates must be sent using approved channels and content templates
- Partner-specific continuity notices must be prepared for:
- Regulatory authorities
- Major enterprise clients
- Cloud service providers

7.4.3.5 Plan Distribution and Accessibility

- The BCP must be:
  - Reviewed and signed off annually by executive leadership
  - Digitally accessible via a secure offline and cloud-based location
  - Available in each global site’s local language (where applicable)

7.4.4 Roles and responsibilities

- **Chief Operating Officer (COO):** BCP owner, responsible for ensuring readiness and cross-departmental integration
- **IT Continuity Manager:** Maintains infrastructure-specific response playbooks
- **Department Heads:** Identify critical workflows and maintain BCP contact lists
- **Communications Lead:** Drafts and disseminates internal/external updates
- **HR Manager:** Handles people continuity, remote work coordination, and relocation planning

7.4.5 Enforcement

Failure to participate in BCP reviews, training, or testing is considered a breach of operational responsibilities and may result in corrective action or management-level escalation. Compliance with the BCP policy is mandatory for all departments.

7.4.6 Reference

- NIST SP 800-53 Rev. 5 (CP-2): Contingency Planning
- ISO 22301:2019 – Business Continuity Management Systems (BCMS)
- ViraShield BIA Framework & Methodology
- Global Facility Redundancy Strategy
- Crisis Communication SOP (ViraShield Internal Document)

8 Specialized Product Security Policies

8.1 Cross-Platform Threat Analytics Policy

Frameworks: NIST SP 800-53 (SI-4), MITRE ATT&CK

Policy #: VS-CTAP-027

Policy Title: Cross-Platform Threat Analytics Policy

Policy Owner: Director of Threat Intelligence

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Specialized Security & Analytics

8.1.1 Purpose

To define how ViraShield Technologies Inc. collects, correlates, and analyzes threat data across supported platforms (Windows, Android, smart TVs, automotive systems, IoT, etc.) to proactively detect and defend against malware, suspicious behaviors, and targeted attacks.

8.1.2 Scope

This policy applies to:

- All platforms where the ViraShield Portable AV device is supported
- Internal AI/ML detection engines, behavior models, and signature generation systems
- Cloud telemetry ingestion pipelines and regional threat correlation nodes
- Employees involved in malware research, telemetry processing, and analytics

8.1.3 Policy Statement

8.1.3.1 Threat Telemetry Collection

- With user consent, anonymized threat logs and system metadata are uploaded to ViraShield's telemetry servers
- Collection includes:
  - Device OS fingerprint
  - AV engine detections and threat family metadata
  - File hashes, system behavior profiles, and sandbox results
- Telemetry data is regionally stored in compliance with GDPR, India DPDP, and PDPA

8.1.3.2 Cross-Platform Behavioral Analysis

- The Threat Intelligence Team will:
  - Use the MITRE ATT&CK framework to map adversary behaviors
  - Detect lateral movements across devices using similar firmware
  - Flag anomalies in behavior consistency across Android, Windows, and IoT clients

8.1.3.3 Signature Development & Distribution

- Detected threats and confirmed zero-days are fed into:
- Automated signature generation modules
- OTA update queues for real-time device updates

- Offline AV engine cache (for devices without connectivity)

8.1.3.4 Intelligence Sharing

- ViraShield will participate in:
  - Private malware exchange alliances
  - National CSIRT collaborations (e.g., US-CERT, CERT-In)
  - Coordinated disclosure programs for threats discovered via telemetry

8.1.3.5 Platform-Specific Threat Monitoring

- AV analytics models will be tuned per platform:
  - Android: Permission abuse, hidden APKs, app behavior
  - Smart TVs: Firmware exploit telemetry, sideloaded apps
  - Automotive systems: USB injection behavior, rogue firmware detection
- Threat coverage gaps will be documented and updated quarterly

8.1.3.6 Data Retention and Review

- Telemetry logs must be:
  - Stored for a maximum of 90 days unless legally extended
  - Analyzed weekly for threat trends and incident indicators
  - Encrypted at rest and in transit using AES-256 and TLS 1.3

8.1.4 Roles and responsibilities

- **Director of Threat Intelligence:** Oversees analytics program, validates correlation logic
- **Telemetry Engineers:** Design collection logic, ensure compliance with regional policies
- **Data Scientists:** Train, tune, and monitor AI detection models
- **Security Research Team:** Confirms zero-days, coordinates external threat feeds
- **Compliance Officer:** Ensures telemetry sharing and storage practices meet legal mandates

8.1.5 Enforcement

Intentional misuse or unauthorized access of telemetry data is considered a critical violation of ViraShield’s internal policy and may result in legal action, revocation of access rights, or termination.

8.1.6 Reference

- NIST SP 800-53 Rev. 5 (SI-4): Information System Monitoring
- MITRE ATT&CK Framework – Enterprise & Mobile Matrices

- GDPR, India DPDP, Singapore PDPA – Telemetry Compliance
- ViraShield AI Detection Engine Design Doc
- ViraShield Regional Logging Policy (INT-RLP-002)

8.2 Device Spoofing and Counterfeit Prevention Policy

Frameworks: NIST SP 800-53 (IA-3), NIST SP 800-207

Policy #: VS-DSCP-028

Policy Title: Device Spoofing and Counterfeit Prevention Policy

Policy Owner: Chief Technology Officer (CTO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Hardware Integrity & Product Security

8.2.1 Purpose

To define the controls and practices used by ViraShield Technologies Inc. to prevent spoofed, cloned, or counterfeit devices from functioning within its product ecosystem. This policy ensures that only authentic, verified USB-based antivirus devices can connect to backend infrastructure and receive updates, reducing risk of supply chain compromise, data exfiltration, or malware injection.

8.2.2 Scope

This policy applies to:

- All ViraShield Portable AV hardware and embedded firmware
- Device identity validation systems within the OTA and license verification platform
- Supply chain operations, manufacturing, QA, and field activation checkpoints
- Product security and firmware engineering teams

8.2.3 Policy Statement

8.2.3.1 Unique Device Identity Enforcement

- Every production device must include a hardware-embedded unique cryptographic identity (e.g., ECC-based keypair or serial-bound hash)
- Device identities are enrolled and validated through secure bootstrapping during manufacturing
- Backend infrastructure must reject any device not registered in the Device Identity Registry (DIR)

8.2.3.2 Counterfeit Detection at Runtime

- Devices must report identity fingerprint and firmware integrity hash at every cloud connection (e.g., for license validation or update check)
- Spoofed, duplicated, or tampered fingerprints will result in an automatic denylisting and license revocation
- Alerts triggered via the SIEM are escalated to the Security Operations Center (SOC)

8.2.3.3 Secure Supply Chain Control

- All contract manufacturers must pass annual compliance audits including review of:
  - Physical security measures
  - Device ID and bootloader configuration logs
  - Chipset sourcing chain
- Tamper-evident seals and epoxy coating are applied post-manufacturing
- Shipping batches are tracked using signed manifests and scanned into the firmware registration system

8.2.3.4 Zero Trust Communication Protocols

- Using guidance from **NIST SP 800-207**, all device-to-cloud communication must include:
  - Enforced mutual TLS
  - Contextual validation (location, time-of-use, firmware hash)
  - Session fingerprinting to detect lateral spoofing behavior

8.2.3.5 Anti-Reverse Engineering Measures

- AV firmware includes the following protections:
- Obfuscated logic and encrypted payloads
- Secure boot enabled at hardware level
- Regular rotating memory layouts (via randomized bootloader mapping)

8.2.3.6 Incident Response for Counterfeit Detection

- Firmware If a counterfeit device is detected in-field:
  - Activation will be rejected in real time
  - Threat intel team will conduct source traceback
  - Supply chain disruption will trigger a mandatory OEM revalidation check
  - Customers will be notified using a security bulletin template

8.2.4 Roles and responsibilities

- **Chief Technology Officer (CTO):** Approves anti-counterfeit strategy and device architecture controls
- **Product Security Team:** Designs integrity verification logic and cryptographic identifiers
- **Firmware QA Lead:** Manages secure firmware deployment and testing for validation logic
- **Supply Chain Manager:** Tracks serials, audits OEMs, and handles authenticity logs
- **SOC Team:** Monitors telemetry for spoofing alerts and blacklists known bad devices

8.2.5 Enforcement

Counterfeit device distribution or internal misuse of device identities is considered a critical violation of company policy and may result in legal investigation, termination, and external reporting to law enforcement or regulators.

8.2.6 Reference

- NIST SP 800-53 Rev. 5 (IA-3): Device Identification and Authentication
- NIST SP 800-207: Zero Trust Architecture
- ViraShield Firmware Signing SOP
- Secure Supply Chain & Batch Certification Framework
- ViraShield Hardware Identity Management System (HIMS)
- OEM Vendor Agreement Terms – Anti-Counterfeit Clause (Appendix C)

8.3 Offline Signature Expiry Policy

Frameworks: NIST SP 800-53 (SI-12), ISO/IEC 27001:2022 (Annex A.14)

Policy #: VS-OSEP-029

Policy Title: Offline Signature Expiry Policy

Policy Owner: Chief Product Officer (CPO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Product Security / Detection Integrity

8.3.1 Purpose

To define ViraShield's policy for expiring and limiting the use of outdated malware signature files on offline devices. This policy ensures that devices relying on cached threat intelligence do not operate beyond a secure window without updates, maintaining AV effectiveness and compliance.

8.3.2 Scope

This policy applies to:

- All ViraShield Portable AV devices operating in offline mode
- Firmware modules handling signature update validation and expiration checks
- Internal malware signature update infrastructure (OTA systems)
- Customer support workflows handling offline activation exceptions

8.3.3 Policy Statement

8.3.3.1 Signature Expiry Enforcement

- Each signature file downloaded via OTA includes a signed expiration timestamp
- Devices must validate the age of the signature cache at boot and periodically during runtime
- If the cached signatures exceed the allowed offline window, the device will enter Limited Scan Mode, displaying an on-screen notification

8.3.3.2 Expiry Threshold Definition

- The default maximum offline signature validity is 30 days from last update
- Device regions subject to higher threat volatility (e.g., APAC, LATAM) may have reduced limits to 14 days
- Firmware shall allow grace period logic of up to 3 days for deferred updates in low-connectivity zones

8.3.3.3 Limited Scan Mode Behavior

- Notifications When in expired state, the AV engine shall:

  - Scan only common malware signatures (core subset)
  - Disable behavioral heuristics that depend on active threat feeds
  - Prompt user to reconnect for update via notification interface

8.3.3.4 User Notification and Logging

- Devices must visibly notify the user of expiry via status light (if embedded) or host screen message
- Expired usage attempts and scans are logged in encrypted local cache and uploaded on next connection

- Support agents reviewing expired logs will flag excessive overdue cases for escalation

8.3.3.5 Exception Handling

- B2B clients with isolated operational environments (e.g., defense systems) may request Policy Exceptions via the ViraShield Compliance Team
- Exceptions must include documented controls for:
  - Internal update staging
  - Physical patch application
  - Offline AV signature lifecycle SOPs

8.3.3.6 Exceptions Compliance and Security Impact

- Expired devices do not meet minimum scanning assurance and are considered non-compliant under company IR standards and partner SLAs
- They are excluded from telemetry uploads and external threat intelligence correlation

8.3.4 Roles and responsibilities

- **Chief Product Officer (CPO):** Owns offline functionality policy and expiry thresholds
- **Firmware Development Lead:** Implements and maintains expiry enforcement logic
- **OTA Platform Manager:** Ensures signature metadata includes valid expiration timestamps
- **Technical Support Team:** Manages customer exception requests and offline troubleshooting
- **Compliance Officer:** Reviews policy exemptions and regulatory impact (GDPR, HIPAA)

8.3.5 Enforcement

Any attempt to disable expiry logic, tamper with signature dates, or distribute expired configurations to customers is a direct violation of security policy. This may lead to termination, blacklisting, or legal escalation.

8.3.6 Reference

- NIST SP 800-53 Rev. 5 (SI-12): Information Output Handling and Retention
- ISO/IEC 27001:2022 – Annex A.14: System Acquisition, Development, and Maintenance
- ViraShield Signature Expiry Implementation SOP
- AV Limited Mode UI Guidelines

- Offline Deployment Exception Request Form (FOR-SEC-047)

8.4 Subscription Lock & Deactivation Policy

Frameworks: NIST SP 800-53 (AC-4, AC-19), Internal Logic

Policy #: VS-SLDP-030

Policy Title: Subscription Lock & Deactivation Policy

Policy Owner: Director of Product Lifecycle Security

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Licensing & Access Control

8.4.1 Purpose

To define the mechanisms through which ViraShield enforces licensing-based access controls, locks devices upon subscription expiration, and disables unauthorized or cloned usage. This ensures that only active, verified, and compliant USB antivirus devices can access advanced features and signature updates.

8.4.2 Scope

This policy applies to:

- All ViraShield Portable AV devices shipped with subscription-based licensing
- Cloud-based license verification infrastructure
- Firmware modules responsible for license enforcement, lockout, and deactivation
- Customer support, licensing, and product security teams

8.4.3 Policy Statement

8.4.3.1 License Validation & Access Enforcement

- Devices must validate active subscription status on first use and every 7 days thereafter (if connected)
- License checks are enforced using a secure API call to ViraShield’s License Validation Service (LVS)
- Expired or revoked licenses result in automatic deactivation of premium features and OTA access

8.4.3.2 Subscription Lockout Mechanism

- Upon expiration or revocation:
  - Device enters Locked Mode

  - Scanning is limited to basic protection using static, pre-cached core signatures
  - The user is prompted to renew via device notification on host screen
- Locked devices are unable to:
  - Perform behavioral scanning
  - Upload telemetry
  - Access firmware updates

8.4.3.3 Auto-Deactivation on Misuse or Fraud

- Devices flagged for:
  - Cloned keys
  - Multi-device sharing
  - Repeated false firmware modification attempts

  … will be remotely deactivated and added to the Device Denylist Registry
- Re-enablement is possible only via internal investigation and secure reactivation workflow

8.4.3.4 Tamper Detection & Forced Lockdown

- Emergency Any attempt to:
  - Override subscription logic
  - Modify firmware activation logic
  - Spoof API calls to LVS

  …will trigger a forced lockout, alerting the SOC and product security

8.4.3.5 Plan Grace Period & Notification

- Customers are provided a **5-day grace period** after expiry
- Notification cadence:
  - Day 1 post-expiry: UI-based warning and email reminder
  - Day 4: Final notice with limited scan warning
  - Day 6: System enters Locked Mode

8.4.3.6 Region-Specific Licensing Enforcement

- Subscription licensing must comply with applicable regional laws (e.g., auto-renewal restrictions in EU)
- Regional licenses may be mapped to localized subscription servers (e.g., EU clients routed via Frankfurt)

8.4.4 Roles and responsibilities

- **Director of Product Lifecycle Security:** Owns policy logic and enforcement thresholds
- **License Infrastructure Engineer:** Maintains LVS and validation protocols
- **Cloud DevOps Team:** Secures the API and handles deactivation payload delivery
- **Support & Licensing Team:** Assists customers with renewals, disputes, and reactivations
- **SOC Analyst:** Investigates lockouts due to tampering or suspicious activity

8.4.5 Enforcement

Use of expired, tampered, or unauthorized license configurations is considered a breach of ViraShield Terms of Use and product agreement. Consequences include full deactivation, support denial, and escalation to legal counsel when required.

8.4.6 Reference

- NIST SP 800-53 Rev. 5 (AC-4): Information Flow Enforcement
- NIST SP 800-53 Rev. 5 (AC-19): Access Control for Mobile Devices
- ViraShield License Validation Service (LVS) Architecture
- Device Denylist Registry Operations Manual
- Regional Licensing Policy Matrix – GDPR/India DPDP Alignment
- Internal Enforcement Logic Specification (ENF-VS-LIC-2025)

9 Regional and Global Compliance Policies

9.1 Global Regulatory Compliance Policy

Frameworks: NIST SP 800-53 (PL-1, RA-3), GDPR, India DPDP, Singapore PDPA

Policy #: VS-GRCP-031

Policy Title: Global Regulatory Compliance Policy

Policy Owner: Chief Compliance Officer (CCO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Legal, Data Protection, Regional Compliance

9.1.1 Purpose

To ensure that ViraShield Technologies Inc. maintains continuous compliance with applicable regional and international data protection laws, cybersecurity regulations, and licensing rules across its operational footprint in over 30 countries. This policy governs how products, infrastructure, and processes align with legal mandates in the U.S., EU, APAC, and LATAM markets.

9.1.2 Scope

This policy applies to:

- All global locations and ViraShield data processing activities
- Customer-facing AV devices and embedded data-handling features
- Internal compliance, legal, and product architecture teams
- Vendors and partners subject to joint compliance requirements
- All data lifecycle processes including collection, transmission, storage, and deletion

9.1.3 Policy Statement

9.1.3.1 Data Privacy Regulations by Region

- European Union:
  - GDPR compliance enforced for telemetry consent, data minimization, user rights
  - Data stored or processed in EU hosted servers (Frankfurt region)
- India:
  - India’s DPDP Act 2023 governs data localization and purpose limitation for telemetry originating from Indian customers
- Singapore & APAC:
  - Compliance with Singapore PDPA and country-specific cybersecurity and cross-border rules (e.g., Malaysia PDP, Japan APPI)
- United States:
  - Adheres to state-specific regulations (e.g., CCPA, HIPAA when integrated with medical AV deployments)

9.1.3.2 Cross-Border Data Transfer Safeguards

- All international transfers use standard contractual clauses (SCCs) or regional equivalents
- Transfers must use end-to-end encryption (TLS 1.3, AES-256) and endpoint validation
- Cross-region failover systems must respect regional storage separation controls

9.1.3.3 Risk Assessments & Regulatory Gap Analysis

- The Compliance Team must perform biannual compliance audits and risk assessments
- All product rollouts must include a jurisdictional impact checklist
- Policy compliance is reviewed during the annual Information Security Management System (ISMS) audit

9.1.3.4 Consent & Opt-In/Opt-Out Enforcement

- ViraShield will participate in:
  - Private malware exchange alliances
  - National CSIRT collaborations (e.g., US-CERT, CERT-In)
  - Coordinated disclosure programs for threats discovered via telemetry

9.1.3.5 Platform-Specific Threat Monitoring

- Devices with optional telemetry must:
  - Display clear opt-in consent upon setup (multi-language compliant)
  - Provide visible option to withdraw consent or disable telemetry features
  - Log user decisions securely and attach device-specific privacy profiles

9.1.3.6 Local Regulatory Liaison Program

- ViraShield will appoint Regional Compliance Officers (RCOs) in high-regulation areas (EU, India, Singapore)
- RCOs serve as points of contact for:
  - Regulatory authorities
  - Customer data subject access requests (DSARs)
  - Breach notifications and reporting mandates

9.1.3.7 Vendor and Third-Party Contractual Alignment

- All vendors must sign data processing agreements (DPAs)
- Contracts must include clauses for:\n
  - Data security controls
  - Breach notification timelines
  - Local compliance certifications

9.1.4 Roles and responsibilities

- **Chief Compliance Officer (CCO):** Owns global regulatory oversight and policy governance

- **Regional Compliance Officers (RCOs):** Enforce local alignment and regulatory reporting
- **Legal Counsel:** Drafts and approves data transfer mechanisms and international contracts
- **Cloud Ops Manager:** Implements geographic routing and regional storage controls
- **Support & Privacy Team:** Responds to DSARs, opt-out requests, and regulatory inquiries

9.1.5 Enforcement

Violations of global compliance requirements may result in severe penalties including regulatory fines, customer litigation, and reputational damage. All departments are required to report non-conformity or legal risk exposure immediately to the CCO.

9.1.6 Reference

- NIST SP 800-53 Rev. 5 (PL-1): Security Planning, (RA-3): Risk Assessment
- GDPR (General Data Protection Regulation) – EU
- India DPDP Act, 2023
- Singapore Personal Data Protection Act (PDPA)
- ISO/IEC 27701: Privacy Information Management
- ViraShield Data Transfer Governance SOP
- Regional Regulatory Impact Tracker – Internal Compliance Portal

10 Hardware Lifecycle Policies

10.1 Hardware Lifecycle Security Policy

Frameworks: NIST SP 800-53 (MP-4, MP-6), NIST SP 800-88, ISO/IEC 27001:2022 (Annex A.11)

Policy #: VS-HLSP-032

Policy Title: Hardware Lifecycle Security Policy

Policy Owner: Director of Hardware Security & Supply Chain Integrity

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Hardware & Device Lifecycle Security

10.1.1 Purpose

To define the security and handling requirements for all stages of the hardware lifecycle at ViraShield Technologies Inc. — from production and delivery to in-field use, retirement, and secure disposal — ensuring the protection of customer data, intellectual property, and supply chain integrity.

10.1.2 Scope

This policy applies to:

- All ViraShield Portable AV devices and hardware components (e.g., USB enclosures, chipsets)
- Development and production hardware used in QA or R&D
- Returned, defective, or end-of-life (EOL) units
- Partner and OEM manufacturing sites handling company hardware
- All departments involved in provisioning, transport, recovery, and destruction of physical devices

10.1.3 Policy Statement

10.1.3.1 Secure Manufacturing Standards

- Devices must be manufactured in facilities audited against ISO/IEC 27001 or equivalent supply chain controls
  - Every device must include:
  - Tamper-evident packaging
  - Epoxy-sealed critical chips
- Signed boot firmware and serial-linked production records
- Firmware images must be flashed using secure, air-gapped environments

10.1.3.2 Asset Tracking and Custody Chain

- Each hardware unit must be assigned a **unique serial and asset ID** at origin
- Movement must be logged through the Hardware Lifecycle Management System (HLMS)
- All touchpoints (R&D, QA, packaging, shipping) must use barcode or RFID scans

10.1.3.3 In-Field Usage Monitoring

- Devices report their lifecycle state (active, near-expiry, flagged for return) as metadata during OTA communication
- Devices not communicating for 60+ days are flagged for expiry review

- Returned or suspicious devices are locked automatically until investigated

10.1.3.4 Secure Return & Reclamation Protocols

- Any hardware returned due to refund, repair, or suspected compromise must be:
    - Logged in the Hardware Recovery Log
    - Wiped via signed firmware routine
    - Tagged with condition code (OK, Tampered, Cloned, Defective)
    - Physically isolated pending assessment

10.1.3.5 End-of-Life (EOL) and Decommissioning

- Devices must follow NIST SP 800-88 media sanitization guidelines before destruction
- Physically destroyed units must be recorded in the EOL Certificate Registry
- Retired hardware with unrecoverable signature engines must be marked “Deactivated” in LVS

10.1.3.6 Internal Hardware Security Controls

- Development and test devices must be physically locked when unattended
- Storage rooms, labs, and loading bays must have:
    - 24/7 access monitoring
    - Role-based physical access control
    - CCTV monitoring (logs retained for 90 days minimum)
- Local compliance certifications

10.1.4 Roles and responsibilities

- **Director of Hardware Security:** Overall accountability for lifecycle management
- **Supply Chain Operations Lead:** Oversees HLMS tracking and logistics
- **Product Security Engineer:** Validates firmware integrity and hardware tamper checks
- **Returns & RMA Manager:** Manages recovery, reclamation, and destruction processes
- **Compliance Auditor:** Conducts biannual reviews of hardware lifecycle policy execution

10.1.5 Enforcement

Failure to comply with hardware tracking, destruction, or tamper control protocols may result in disciplinary action, breach response, or supplier disqualification. Any device found in unauthorized use will be locked, investigated, and reported under IR policy.

10.1.6 Reference

- NIST SP 800-53 Rev. 5:
- MP-4: Media Storage
- MP-6: Media Sanitization
- NIST SP 800-88: Guidelines for Media Sanitization
- ISO/IEC 27001:2022 (Annex A.11) – Equipment Security
- ViraShield Secure Hardware Manufacturing SOP
- HLMS (Hardware Lifecycle Management System) Logs
- AV RMA Return & Certification Process Documentation

10.2 Supply Chain Security Policy

Frameworks: NIST SP 800-161, ISO/IEC 27001:2022 (Annex A.15)

Policy #: VS-SCSP-033

Policy Title: Supply Chain Security Policy

Policy Owner: Chief Supply Chain Security Officer (CSCSO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Supply Chain Risk Management (SCRM) & Vendor Integrity

10.2.1 Purpose

To establish and enforce security controls throughout ViraShield’s global supply chain, ensuring that all hardware components, embedded firmware, manufacturing partners, and logistics pathways adhere to strong integrity, confidentiality, and resilience standards to prevent supply chain attacks and maintain device trustworthiness.

10.2.2 Scope

This policy applies to:

- All OEM, ODM, and third-party hardware manufacturing partners
- Component suppliers (e.g., microcontrollers, memory, USB enclosures)
- Shipping vendors and regional logistics providers

- Internal supply chain and vendor risk management teams
- All systems tracking sourcing, transport, integration, and final device deliver

10.2.3 Policy Statement

10.2.3.1 Vendor Risk Assessment and Qualification

- All vendors must pass a pre-contract due diligence review that includes:
  - Background check for nation-state exposure or previous breaches
  - Review of third-party SOC 2, ISO 27001, or cybersecurity certification
  - Signed Supply Chain Integrity Agreement (SCIA) with ViraShield
  - Vendors must renew qualification annually

10.2.3.2 Secure Sourcing of Components

- Components must be procured from:
  - Whitelisted suppliers with traceable origin (no gray market chips)
  - Vendors that commit to bill-of-materials (BoM) transparency
  - Any change in supplier or hardware revision requires pre-approval by the Product Security Office

10.2.3.3 Chain of Custody and Transit Security

- Devices and components must maintain end-to-end traceability in the Supply Chain Intelligence Platform (SCIP)
- All shipping logs must include:
  - Serial IDs
  - Timestamped checkpoints
  - Condition scan results at each handoff
- High-value shipments must include tamper-evident seals and GPS-based shipment monitoring

10.2.3.4 Firmware & Configuration Integrity

- Firmware must be:
  - Digitally signed and hashed before loading onto devices
  - Flashable only in secure rooms with air-gapped tooling
  - Devices will not pass QA if firmware integrity check fails

10.2.3.5 Third-Party Security Controls Monitoring

- Suppliers must undergo periodic:
  - Vulnerability exposure scanning (NIST CVE tracking)
  - On-site audits by the Supply Chain Audit Team (SCAT)

    - Penetration testing of partner staging environments (if hosting configuration scripts)

10.2.3.6 Response to Supply Chain Incidents

- If any supply chain compromise or counterfeit exposure is detected:
    - The batch must be quarantined in quarantine inventory status
    - SOC and Legal must be notified within 24 hours
    - Incident reviewed by CSCSO and corrective action issued
    - Affected customers are informed via Tier 1 product advisory

10.2.4 Roles and responsibilities

- **Chief Supply Chain Security Officer (CSCSO):** Owns supply chain risk governance and partner enforcement
- **Procurement Risk Manager:** Conducts assessments, tracks compliance scores
- **Product Security Team:** Approves secure configurations and firmware assurance
- **Logistics Compliance Coordinator:** Ensures custody logs and shipping integrity
- **Vendor Audit Lead:** Manages on-site audits, contract compliance, and SCIA enforcement

10.2.5 Enforcement

Vendors or staff found violating supply chain security policy or involved in unauthorized component substitution, breach concealment, or tampering will face contract termination, legal escalation, and potential civil liability. Internal employees may face disciplinary action up to termination.

10.2.6 Reference

- NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- ISO/IEC 27001:2022 (Annex A.15) – Supplier Relationships
- ViraShield Supply Chain Integrity Agreement (SCIA)
- SCIP Log Management Framework
- Firmware Signing SOP (FRMW-SGN-OPS-022)
- Global Risk Scorecard for Component Origin Tracking

11 Threat Intelligence, AI, and Engine Policies

11.1 Antivirus Detection Engine Development Policy

Frameworks: NIST SP 800-83, ISO/IEC 27034 27001:2022 (Annex A.11)

Policy #: VS-ADED-034

Policy Title: Antivirus Detection Engine Development Policy

Policy Owner: Director of AI Threat Detection Engineering

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Secure Software Development & Threat Detection

11.1.1 Purpose

To establish secure development standards, validation protocols, and deployment procedures for the proprietary antivirus (AV) detection engine embedded in ViraShield Portable AV devices. This policy ensures that detection models, rulesets, and signature generation processes maintain effectiveness, reliability, and resistance to tampering or evasion.

11.1.2 Scope

This policy applies to:

- All developers and engineers involved in AV engine development
- Threat research teams responsible for behavioral detection logic
- Signature generation and classification pipelines (manual & automated)
- On-device and cloud-assisted AV architecture
- OTA update and validation routines related to the AV engine

11.1.3 Policy Statement

11.1.3.1 Secure Engine Architecture

- The antivirus engine must follow modular design principles and include:
  - Static signature scanner
  - Heuristic behavior model
  - AI/ML anomaly detection module
- Each module must operate independently, and report results to a unified correlation system
- Firmware embedding the engine must enforce Secure Boot and signed updates only

11.1.3.2 Signature & Heuristic Development

- Signature creation must be based on:
  - Malware reverse engineering
  - Behavioral sandboxing (e.g., mutex detection, process injection patterns)
  - Crowd-sourced telemetry analysis
- All signatures must be:
  - Cryptographically signed
  - Version-controlled in a secure repository
  - Subjected to regression testing against benign samples (false-positive control)

11.1.3.3 Machine Learning and AI Model Management

- All AI models used in detection (e.g., for zero-day classification) must:
  - Be explainable (XAI-ready) and include version metadata
  - Undergo fairness and bias assessment
  - Be trained on malware corpora cleared through legal, clean-room environments
- Retraining must occur quarterly or sooner based on threat trends

11.1.3.4 Testing and Simulation

- Every detection rule must be tested using:
  - Known-good testbeds (AMTSO guidelines)
  - Simulated evasive malware (e.g., packers, polymorphic payloads)
- The AV engine must pass:
  - False positive threshold (below 0.01%)
  - Detection efficacy threshold (above 98%) before release

11.1.3.5 OTA Deployment and Verification

- Updated engines are distributed via signed OTA updates through TLS 1.3
- Devices must verify digital signatures before applying engine updates
- Rollback protection logic must prevent downgrade to vulnerable engine builds

11.1.3.6 Incident Response Linkage

- In the event of a malware detection failure (e.g., zero-day evasion), the AV engine team must:
  - Log a root cause analysis (RCA)
  - Issue hotfix signatures within 24–48 hours

  - Coordinate with the SOC and Threat Intelligence Team for retrospective coverage

11.1.4 Roles and responsibilities

- **Director of AI Threat Detection Engineering:** Owns architecture, training standards, and model governance
- **Detection Engineers:** Create and validate rules, ensure regression-safe releases
- **Data Science Team:** Trains and tunes behavioral and ML-based detection models
- **QA and Security Research Analysts:** Conduct simulation testing, signature stress tests
- **OTA Delivery Lead:** Manages signed update propagation and rollback safeguards

11.1.5 Enforcement

Any unauthorized modification of detection engines, use of unvetted signatures, or deployment bypass is a critical violation. Violators may be terminated and referred to internal audit and incident response teams.

11.1.6 Reference

- NIST SP 800-83: Guide to Malware Incident Prevention and Handling
- ISO/IEC 27034: Application Security Framework
- AMTSO Guidelines – Testing and Evaluation of Antivirus Products
- ViraShield OTA Distribution & Rollback SOP
- Secure Firmware Boot Architecture – Internal Engineering Doc
- AV Engine Git Repository Access Policy

11.2 Antivirus Scanning Behavior Policy

Frameworks: AMTSO Standards, Internal Logic

Policy #: VS-ASBP-035

Policy Title: Antivirus Scanning Behavior Policy

Policy Owner: Director of Threat Detection & Engine Runtime

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Runtime Detection, UX & Performance Security

11.2.1 Purpose

To define the scanning modes, behavioral thresholds, exclusion criteria, and user-impact tolerances for the embedded antivirus engine within ViraShield Portable AV devices, ensuring optimized real-time detection while maintaining usability, platform compatibility, and system performance across supported devices.

11.2.2 Scope

This policy applies to:

- All portable USB-based antivirus devices distributed by ViraShield
- Engine behavior across host platforms (Windows, macOS, Android, Smart TVs, vehicle systems)
- Device runtime behavior (on-access scanning, full scan, contextual analysis)
- Customer-experience and UX consistency across global firmware versions
- Integration with host systems that have limited resources or security policies

11.2.3 Policy Statement

11.2.3.1 Scan Mode Behavior by Default

- Upon insertion, the ViraShield device initiates:
  - On-Access Scanning: Actively monitors file operations (open, execute, modify)
  - Initial Rapid Scan: Runs within the first 90 seconds to detect dormant malware
- Smart Scanning logic adapts scan depth based on:
  - Host CPU availability
  - OS type and threat signature priority
  - User interaction (e.g., USB is idle or actively navigating files)

11.2.3.2 Behavioral Detection Triggers

- The scanning engine uses behavior-based rules to flag:
  - Abnormal process trees
  - Memory injection patterns
  - Encryption loops (ransomware behavior)
- Suspicious outbound connections or DNS tunneling
- Detections must be verified against false positive suppression logic using a weighted confidence score

11.2.3.3 Scan Scope & Heuristics

- Full disk or directory scans must exclude:
  - Host antivirus or EDR cache folders
  - Secure OS directories (root/system unless explicitly authorized)
- Heuristic depth is tiered:
  - Basic: Static checksums, known patterns
  - Intermediate: API call mapping, entropy analysis
  - Advanced: Code emulation, AI behavior chaining (on supported hosts)

11.2.3.4 Firmware & Configuration Integrity

- Firmware must be:
  - Digitally signed and hashed before loading onto devices
  - Flashable only in secure rooms with air-gapped tooling
  - Devices will not pass QA if firmware integrity check fails

11.2.3.5 UX and Performance Guardrails

- The device must not:
  - Degrade system performance beyond 10% CPU/memory usage
  - Interrupt user sessions (no forced popups unless severe threat is detected)
  - Display duplicate warnings already issued by host AV (where integrated)
- Scanning runs sandboxed within the device and does not install any host agents

11.2.3.6 Mode Transitions & Overrides

- Safe Mode: Triggered on unsupported hosts — limits to read-only, static signature scan
- Silent Mode: Activated during gaming/video playback — suppresses UI but logs detections
- Manual Override: Users can enable full recursive scan via host UI widget (if supported)

11.2.3.7 Platform-Specific Constraints

- Android:
  - Must prompt user to grant storage scanning permissions
  - Uses intent-based analysis for APKs
- Smart TVs:

  - Scans app storage and sideloaded binaries only
  - Suppresses alerts unless malicious signature is confirmed

11.2.4 Roles and responsibilities

- **Director of Threat Detection & Engine Runtime:** Defines scan logic and risk models
- **UX and Product Testing Lead:** Validates user impact and usability consistency
- **Mobile Platform Engineers:** Ensure behavior integrity across Android/TV/IoT
- **Customer Experience Team:** Provides feedback loop from end users for scan behavior tuning
- **Telemetry Analysis Team:** Monitors scan results and anomaly trends for further refinement

11.2.5 Enforcement

Deviations from approved scan behavior, performance constraints, or failure to suppress known false positives must be remediated through a hotfix. Recurring violations may result in rollback or feature disablement across firmware branches.

11.2.6 Reference

- AMTSO Guidelines: Testing and Evaluation of Malware Detection Systems
- ViraShield Internal Detection Logic Spec v3.2
- Platform Runtime Behavior Matrix (Windows, Android, TV, Automotive)
- User Feedback Digest & Performance Baseline Logs
- OTA Safe Mode Trigger Configuration File
- UX Flowchart for Threat Notifications

11.3 AI/ML Model Security Policy

Frameworks: NIST SP 800-53 (SA-15), ISO/IEC 27034)

Policy #: VS-AMLSP-036

Policy Title: AI/ML Model Security Policy

Policy Owner: Chief Data Scientist

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Threat Detection, AI Safety, Model Governance

11.3.1 Purpose

To define security, integrity, training, deployment, and lifecycle controls for artificial intelligence (AI) and machine learning (ML) models used in ViraShield's antivirus detection engine. This policy ensures the trustworthiness, robustness, and explainability of all AI/ML implementations that inform real-time malware detection and behavioral threat classification.

11.3.2 Scope

This policy applies to:

- AI/ML models used in the ViraShield Portable AV device's detection engine
- Cloud-assisted AI modules supporting signature generation and anomaly detection
- All employees involved in model design, training, testing, and deployment
- Datasets, inference pipelines, retraining processes, and model drift tracking
- On-device models (embedded inference) and cloud-hosted augmentations

11.3.3 Policy Statement

11.3.3.1 Model Development & Design Controls

- All AI/ML models must be developed in accordance with:
  - Secure Software Development Lifecycle (SSDLC) standards
  - Adversarial risk mitigation principles (e.g., evasion, poisoning)
- Developers must maintain:
  - Source code versioning
  - Model configuration metadata
  - Explainability metadata (e.g., SHAP, LIME artifacts)

11.3.3.2 Dataset Security and Compliance

- Training datasets must be:
  - Acquired ethically and lawfully from verified malware corpora or proprietary threat telemetry
  - Stored in access-controlled, encrypted environments
  - Labeled using internal schema vetted by senior malware analysts
- Personally identifiable information (PII) must be redacted from any user-generated logs used in training

11.3.3.3 Model Validation and Testing

- Before deployment, models must pass:

  - Accuracy threshold ≥ 95% across validation sets
  - False positive rate ≤ 0.01% for clean files
  - Robustness tests (e.g., evasion attacks, adversarial inputs)
- A Model Risk Evaluation Form must be completed and approved by QA and legal before production use

11.3.3.4 Deployment & Runtime Security

- Deployed models must be:
  - Digitally signed and verified at runtime
  - Deployed in a sandboxed inference environment within the firmware
  - Immutable during session (model tampering detection enabled)

11.3.3.5 Model Update and Drift Management

- Models must be retrained:
  - Quarterly, or
  - On urgent basis when zero-day patterns or model drift is observed
- Telemetry-assisted drift indicators must trigger internal alerts
- Updated models must follow peer-review + A/B testing before full rollout

11.3.3.6 Bias & Fairness Assurance

- Models must be reviewed for:
  - Dataset bias (e.g., region-specific malware imbalance)
  - Unintended penalization of benign applications
  - Discriminatory output in cross-platform scanning scenarios
- Reports must be logged in the AI Model Fairness & Bias Register

11.3.4 Roles and responsibilities

- **Chief Data Scientist:** Owns AI/ML development governance and integrity assurance
- **Model Development Engineers:** Train and test models, manage datasets
- **Threat Intelligence Team:** Validate ground truth labels and threat behaviors
- **AI Ethics & Fairness Analyst:** Conduct bias analysis and documentation
- **Cloud Infrastructure Lead:** Secures and monitors inference endpoints

11.3.5 Enforcement

Use of unverified AI/ML models or unauthorized retraining/deployment constitutes a policy violation. Offenses may result in revocation of access, rollback of model updates, or disciplinary review depending on severity and risk impact.

11.3.6 Reference

- NIST SP 800-53 Rev. 5 (SA-15): Development Process, Standards, and Tools
- ISO/IEC 27034: Application Security Framework
- ViraShield AI/ML Lifecycle Governance SOP
- AMTSO Behavior Detection Testing Standards
- AI Bias and Fairness Assessment Workbook
- Secure Model Inference Pipeline Design (INT-AML-ENGINE-004)

11.4 Threat Intelligence Sharing & Signature Update Policy

Frameworks: NIST SP 800-150, ISO/IEC 27001:2022 (Annex A.13)

Policy #: VS-TISUP-037

Policy Title: Threat Intelligence Sharing & Signature Update Policy

Policy Owner: Director of Threat Intelligence & Detection Operations

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Threat Intelligence Collaboration & Signature Management

11.4.1 Purpose

To define the procedures, frequency, integrity, and scope of threat intelligence sharing and malware signature update distribution within ViraShield's ecosystem, ensuring that customers receive real-time protection from emerging threats while maintaining compliance with global information exchange laws and industry best practices.

11.4.2 Scope

This policy applies to:

- ViraShield's AI-assisted threat detection systems
- Cloud-based telemetry correlation engines
- OTA (Over-the-Air) update infrastructure
- Partner threat intelligence exchange channels
- All internal employees managing signature development, testing, approval, and distribution

11.4.3 Policy Statement

11.4.3.1 Threat Intelligence Collection & Processing

- Intelligence is collected from:
  - In-field telemetry logs (with user consent)
  - Public and private threat feeds (e.g., US-CERT, MITRE, commercial partners)
  - Malware honeypots and sandbox analysis systems
- All threat intelligence must be:
  - Parsed using internal correlation engines
  - Tagged with malware family, behavior class, and risk severity
  - De-identified to remove personal or customer-specific information

11.4.3.2 Intelligence Sharing Channels

- ViraShield may share threat intelligence with:
  - National CERTs and global CSIRT alliances
  - Trusted commercial malware consortiums (under NDA)
  - Industry-specific ISACs (Information Sharing and Analysis Centers)
- Shared data must comply with:
  - GDPR, India DPDP, CCPA, PDPA, and local privacy laws
  - ViraShield's internal Cross-Jurisdictional Disclosure Policy

11.4.3.3 Signature Generation & Review

- New malware detections must undergo:
  - Verification via sandbox or reverse engineering
  - Behavior mapping aligned with MITRE ATT&CK
  - QA regression testing (0.01% max FP rate)
- Generated signatures must be:
  - Encrypted and signed using SHA-512 + ECC
  - Tagged with TTL, detection confidence, and severity
  - Uploaded to the Signature Repository (SIG-REPO-CORE)

11.4.3.4 OTA Signature Update Distribution

- Signature updates are pushed:
  - Daily, or hourly in active outbreak scenarios
  - Via TLS 1.3 encrypted OTA channels
  - With rollback metadata and differential update compression

- Devices offline for >30 days enter signature expiry state and notify user for renewal

11.4.3.5 Zero-Day and High-Severity Threat Escalation

- Zero-day detections or critical CVEs must be:
  - Flagged as "Priority 1" by the Threat Intel team
  - Shared with national CERT (e.g., US-CERT, CERT-In) within 48 hours
  - Patched via emergency OTA queue
  - Logged in the Zero-Day Register (ZDR)

11.4.4 Roles and responsibilities

- **Director of Threat Intelligence & Detection Operations:** Owns signature pipeline, vendor feeds, and CERT coordination
- **Threat Correlation Engineers:** Aggregate feeds, tune matching logic, prioritize outbreaks
- **QA Team:** Conduct false positive/negative regression testing
- **OTA Delivery Specialist:** Schedules global rollouts and regional mirror syncs
- **Privacy Compliance Officer:** Ensures data sharing aligns with jurisdictional regulations

11.4.5 Enforcement

Deliberate bypass of threat validation, improper sharing of sensitive data, or signature manipulation without approval will be treated as a critical offense. Incidents will be escalated to Legal, CISO, and external regulators (if required).

11.4.6 Reference

- NIST SP 800-150: Guide to Cyber Threat Information Sharing
- ISO/IEC 27001:2022 Annex A.13 – Communications Security
- MITRE ATT&CK Mapping Framework
- GDPR / India DPDP / CCPA – Privacy Laws Overview
- OTA Signature Pipeline Architecture (DOC-ID: VS-OTA-TIS-006)
- Cross-Jurisdictional Disclosure Control SOP
- Zero-Day Threat Response Procedure (ZDRP-004)

12 OTA and System Resilience Policies

12.1 Firmware Update Rollback Protection Policy

Frameworks: NIST SP 800-193

Policy #: VS-FURPP-038

Policy Title: Firmware Update Rollback Protection Policy

Policy Owner: Director of Firmware Engineering

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Firmware Integrity & System Resilience

12.1.1 Purpose

To define security mechanisms and validation controls that prevent unauthorized or outdated firmware versions from being reinstalled on ViraShield's hardware devices. This policy ensures that once a device receives an authenticated firmware update, it cannot be downgraded to a potentially vulnerable version, preserving system integrity and resilience.

12.1.2 Scope

This policy applies to:

- All ViraShield Portable AV devices with OTA firmware support
- The embedded bootloader and secure update subsystem
- On-device version comparison logic and update handlers
- Engineering, QA, and OTA deployment teams
- Global firmware version registries and rollback prevention records

12.1.3 Policy Statement

12.1.3.1 Secure Boot and Anti-Rollback Enforcement

- All devices must use Secure Boot with cryptographically signed firmware
- A monotonic firmware version counter (FW_VER_ID) must be embedded in each image
- The device must reject any update with a version number lower than the current one

12.1.3.2 OTA Update Verification

- Firmware updates must be:
  - Signed using ECC-based digital signatures

  - Delivered over TLS 1.3 encrypted channels
  - Verified for authenticity and version integrity before installation
- The update process must log version info in the Firmware Audit Log (FAL)

12.1.3.3 Downgrade Attack Prevention

- Any attempt to flash an older version must:
  - Trigger a rollback prevention alert
  - Log a security incident on the device
  - Notify the OTA server (if connected) for centralized audit tracking

12.1.3.4 Bootloader Integrity Protection

- The bootloader must be locked to accept only signed update packages
- Recovery mode must enforce rollback protection policies identically
- Devices must use write-once EFUSE or TPM counters to prevent manipulation

12.1.3.5 Firmware Version Registry Management

- The OTA system must maintain a Global Firmware Version Registry (GFVR)
  - Each release is versioned and timestamped
  - Emergency revocation of compromised versions must be supported
- Devices offline for >90 days must validate version expiration with cloud before applying updates

12.1.3.6 Testing and Validation

- All firmware builds must be:
- Scanned for downgrade vulnerabilities
- Tested on emulator and physical hardware for boot stability
- Reviewed by the **Firmware Security Council (FSC)** before OTA release

12.1.4 Roles and responsibilities

- **Director of Firmware Engineering:** Oversees anti-rollback logic, FW registry, and bootloader protections
- **OTA Systems Engineer:** Validates version counters, logs rollbacks, distributes approved packages
- **Firmware QA Team:** Runs downgrade simulation tests and firmware integrity checks
- **Security Research Team:** Conducts firmware exploit analysis and monitors rollback attempts

- **Compliance Auditor:** Ensures rollback mechanisms align with resilience standards (e.g., NIST SP 800-193)

12.1.5 Enforcement

Bypassing or disabling rollback protection constitutes a security violation. Engineers or vendors who modify bootloader protections or introduce unsigned images into production will be subjected to disciplinary review or termination of contract. Firmware violating rollback policies will be blacklisted in the GFVR.

12.1.6 Reference

- NIST SP 800-193: Platform Firmware Resiliency Guidelines
- ViraShield Secure Boot & Update Architecture (SBUA-005)
- OTA Rollback Protection Implementation Manual
- GFVR (Global Firmware Version Registry) Specification
- Firmware Security Council (FSC) Charter
- Device Root-of-Trust Design Documentation

12.2 Secure OTA Update Validation Policy

Frameworks: ISO/IEC 27001:2022 (Annex A.14 – System Acquisition, Development & Maintenance)

Policy #: VS-SOTAVP-039

Policy Title: Secure OTA Update Validation Policy

Policy Owner: Director of Embedded Systems Security

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Firmware Security & System Maintenance

12.2.1 Purpose

To ensure that all over-the-air (OTA) firmware, antivirus engine, and signature updates deployed to ViraShield products are authenticated, validated, tamper-proof, and comply with cryptographic integrity and performance assurance before being accepted and applied on the device.

12.2.2 Scope

This policy applies to:

- All OTA-based updates for firmware, malware detection engines, or threat signature files

- Embedded security systems in the ViraShield Portable AV product line
- Cloud-side distribution infrastructure and device-side update agents
- Engineering, QA, DevSecOps, and release management personnel

12.2.3 Policy Statement

12.2.3.1 Update Package Creation & Signing

- All OTA packages (firmware and detection updates) must be:
  - Assembled via the OTA Build Signing Pipeline (OBSP)
  - Digitally signed using ECC (Elliptic Curve Cryptography) or RSA 4096-bit private keys
  - Assigned a unique Package UID, timestamp, and SHA-512 hash
  - Versioned with a monotonic ID for rollback prevention (see Policy 12.1)

12.2.3.2 Secure Transmission and Delivery

- OTA updates must be:
  - Delivered over TLS 1.3 or newer with forward secrecy
  - Hosted only on geographically restricted CDN nodes with regional data protection compliance
  - Encrypted at rest prior to endpoint download

12.2.3.3 Device-Side Validation Requirements

- Full Upon receiving an update, the ViraShield device must:
  - Validate digital signature using onboard trusted public key
  - Verify package version > current version (anti-downgrade)
  - Perform hash integrity check before applying the update
  - Check compatibility with device platform and model ID

12.2.3.4 Update Isolation and Rollback Testing

- OTA updates must be:
  - Installed within a sandboxed memory partition
  - Tested for failure recovery (rollback or factory mode fallback)
  - Trigger an alert on checksum mismatch, expired certificate, or failed dependency check

12.2.3.5 Update Validation Lifecycle and Metrics

- Validation success/failure rates are logged in the OTA Compliance Report Registry (OCRR)

- Any update package with <98% install success or >0.01% failure on any platform must be quarantined
- Security regression testing must occur at the firmware and engine level prior to rollout
- For region-specific updates, local compliance verification (e.g., PDPA, DPDP) must be documented

12.2.4 Roles and responsibilities

- **Director of Embedded Systems Security:** Oversees signing authority, key rotation, and trust anchors
- **Firmware Release Engineer:** Builds and packages OTA updates, verifies metadata integrity
- **QA & Regression Testing Team:** Runs platform-specific OTA simulations and vulnerability testing
- **OTA Delivery Coordinator:** Manages distribution, monitors CDN logs, tracks update success rates
- **Compliance & Audit Lead:** Verifies international cryptographic regulations and retention of signing logs

12.2.5 Enforcement

Unauthorized OTA package signing, key misuse, update skipping, or bypassing validation processes will result in incident classification under firmware integrity violations. All affected updates will be revoked, and responsible personnel will be referred for internal investigation.

12.2.6 Reference

- ISO/IEC 27001:2022 Annex A.14 – Secure System Change Management
- OTA Signing Pipeline Security Framework (DOC ID: VS-OBSP-04.7)
- TLS 1.3 Cryptographic Transport Guidelines
- OTA Rollback Fallback Procedure
- OTA Compliance Report Registry (OCRR) Logs
- Key Management Policy (see Policy 6.2)

12.3 Signature Downgrade Detection & Expiry Alert Policy

Frameworks: Internal Logic

Policy #: VS-SDDEA-040

Policy Title: Signature Downgrade Detection & Expiry Alert Policy

Policy Owner: Director of AV Signature Infrastructure

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Threat Signature Integrity & Offline Resilience

12.3.1 Purpose

To establish controls for detecting unauthorized or accidental downgrades of malware signature files on ViraShield AV devices, and to notify users when signature databases are approaching or have reached expiration thresholds due to prolonged offline usage. This ensures scanning remains accurate, trustworthy, and responsive to emerging threats.

12.3.2 Scope

This policy applies to:

- All ViraShield devices utilizing on-device malware signature files
- The firmware module responsible for version control and expiry validation
- Users operating the device in **offline** or **low-connectivity** environments
- QA, detection engine, and OTA update personnel

12.3.3 Policy Statement

12.3.3.1 Signature Version Integrity

- Every downloaded signature package includes:
  - A monotonic version number (SIG_VER)
  - A cryptographic timestamp and digital signature
  - Devices must store the highest verified SIG_VER applied and reject older versions
  - All signature installations must be logged in the Signature Audit Log (SAL)

12.3.3.2 Downgrade Detection Logic

- If a signature file with a lower SIG_VER than current is detected:
  - The system must abort the load and issue a “Downgrade Attempt Blocked” log entry
  - The device must notify OTA services (if online)
  - A rollback alert must be written to internal logs and displayed to the user (if screen is present)

12.3.3.3 Expiry Monitoring and Alerts

- Each signature file includes a **validity period** (e.g., 30 days post-download)
- If the current signature is:
  - **25+ days old**: Soft warning shown
  - **30+ days old**: Scanning enters **Limited Protection Mode**
  - **45+ days old:** Scanning is restricted to low-risk operations; urgent renewal advised
- Devices without displays must issue alerts through host device notifications (where integration is supported)

12.3.3.4 Offline Signature Resilience

- Devices unable to connect for updates must:
  - Cache and use the last known good signature
  - Retain scanning ability for basic known malware
  - Continue to log signature status for audit purposes

12.3.3.5 Testing and Simulation Protocols

- Firmware must simulate downgrade attempts and signature expiry behavior in regression testing
- Quarterly testing must validate expiry alerts, version comparisons, and offline behavior logic
- Results stored in the Signature Expiry Validation Tracker (SEVT)

12.3.4 Roles and responsibilities

- **Director of AV Signature Infrastructure:** Defines expiry parameters, rollback logic, and alert thresholds
- **Firmware Developers:** Implement signature version enforcement and UI alerts
- **QA and Device Simulation Team:** Test downgrade conditions, validate alert workflows
- **OTA Operations Lead:** Monitors stale device update stats, triggers renewal reminders
- **Support & Customer Communication Team:** Informs users of expired signature risks and renewal steps

12.3.5 Enforcement

If rollback or expiration enforcement is disabled, bypassed, or tampered with, such behavior will be escalated as a security integrity violation. Devices found with stale or downgraded signatures beyond tolerance will be flagged in the telemetry backend and locked from full protection mode.

12.3.6 Reference

- ViraShield OTA Signature Lifecycle Specification (DOC-VS-SIGLIFE-021)
- Internal Signature Expiry Parameter Matrix
- Signature Audit Log Design & Retention SOP
- Secure AV Firmware Logic Stack Overview
- Signature Expiry Validation Tracker (SEVT) Reports

12.4 Embedded Device Internet Communication Policy

Frameworks: NIST SP 800-213

Policy #: VS-EDICP-041

Policy Title: Embedded Device Internet Communication Policy

Policy Owner: Director of Embedded Networking Security

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Embedded Network Security & IoT Compliance

12.4.1 Purpose

To define the conditions, protocols, security requirements, and endpoint management standards for internet communications initiated by ViraShield’s embedded antivirus devices. This policy ensures that all network transmissions comply with zero-trust principles, are properly encrypted, and support both privacy and availability requirements across jurisdictions.

12.4.2 Scope

This policy applies to:

- All embedded devices (USB-based AV products) developed by ViraShield
- Outbound communication with ViraShield’s cloud infrastructure, CDNs, or telemetry systems
- Firmware update checks, license key validation, and threat intelligence uploads
- Internal teams responsible for embedded systems, network infrastructure, and telemetry services

12.4.3 Policy Statement

12.4.3.1 Communication Triggers & Use Cases

- ViraShield embedded devices may initiate internet communication only for:
  - License Key Validation (on plugin or renewal trigger)
  - OTA Firmware & Signature Updates (per schedule or critical patch)
  - Telemetry Uploads (with user consent)
  - Cloud Threat Feed Lookup (real-time hash verification if supported)

12.4.3.2 Protocol & Transport Security

- All outbound communications must:
  - Use TLS 1.3 or higher with mutual authentication (certificate pinning enabled)
  - Restrict connections to whitelisted domains and IP ranges defined in the firmware
  - Employ fallback-free DNS to prevent downgrade or hijack attempts

12.4.3.3 Endpoint Access Control

- Devices may only connect to:
- ViraShield's authorized regional cloud nodes (hosted on AWS & Azure)
- Backup update mirrors with signed certs and known domain fingerprints
- DNS and IP routing must be verified before session initiation
- IP reputation lookups must occur quarterly on all endpoint domains

12.4.3.4 Data Minimization & Privacy Compliance

- All outbound data must be:
  - Anonymized before upload unless user is licensed and opted in
  - Limited to essential operational metadata (firmware version, threat hash, device type)
  - Regional upload nodes must be selected based on customer location and data sovereignty laws (e.g., GDPR, DPDP, PDPA)

12.4.3.5 Offline Mode Behavior

- Devices unable to access the internet must:
  - Operate using last-known-good signature sets
  - Retry secure connection once per configured interval (default: 12 hours)
  - Defer any telemetry or updates until secure channel is established

12.4.3.6 Secure Communication Architecture Compliance

- All implementations must meet the requirements outlined in:
- NIST SP 800-213: IoT Device Cybersecurity Guidance
- ViraShield’s Secure Embedded Networking Stack (SENS) specification
- ViraShield’s Geo-aware Endpoint Controller logic

12.4.4 Roles and responsibilities

- **Director of Embedded Networking Security:** Owns policy, endpoint rules, and SENS roadmap
- **Firmware Networking Engineers:** Implement secure connection handlers and domain whitelists
- **OTA Delivery Ops Team:** Maintains availability of mirror nodes and CDN endpoint uptime
- **Privacy & Compliance Officer:** Ensures lawful handling of user metadata per region
- **Threat Intelligence Integration Lead:** Supports secure real-time query logic for cloud-assisted detections

12.4.5 Enforcement

Any device attempting unauthorized outbound connections, bypassing domain validation, or violating the internet access rule set will be automatically locked from OTA services. Violations by staff or vendors will result in investigation and potential revocation of development access credentials.

12.4.6 Reference

- NIST SP 800-213: IoT Device Cybersecurity Guidance
- TLS 1.3 Deployment Handbook – IETF
- ViraShield Secure Embedded Networking Stack (SENS)
- Regional Data Protection Mapping Matrix (EU, US, APAC)
- Embedded DNS and IP Validation Rulebook
- Secure Endpoint Whitelist List v5.4 (WHL-ED-041)

13 Internal Monitoring and Regional Data Protection

13.1 Physical Tamper Response Policy

Frameworks: NIST SP 800-161 (PE-3, PE-6)

Policy #: VS-PTRP-042

Policy Title: Physical Tamper Response Policy

Policy Owner: Director of Hardware Security Engineering

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Hardware Integrity, Supply Chain & Facility Security

13.1.1 Purpose

To establish physical security detection and incident response requirements when tamper attempts or hardware compromise are detected on ViraShield's portable AV products, production hardware, or within facility infrastructure. This policy enforces defense mechanisms, sensor thresholds, and secure destruction protocols in compliance with federal supply chain guidance.

13.1.2 Scope

This policy applies to:

- ViraShield Portable AV devices with tamper-evident and tamper-resistant hardware
- Secure manufacturing lines, packaging, and logistics environments
- Tamper logging subsystems embedded in firmware
- R&D facilities and high-assurance zones under PE-3 and PE-6 controls
- Physical security incidents involving personnel or equipment

13.1.3 Policy Statement

13.1.3.1 Tamper-Resistant Device Design

- All production hardware must:
  - Be built with epoxy-filled chips, sealed casings, and sensor-backed secure enclaves
  - Integrate physical tamper detection circuits capable of logging intrusion events
  - Employ tamper-evident labeling and serialized packaging for shipment traceability

13.1.3.2 On-Device Tamper Detection and Logging

- If a tamper sensor is triggered, the device must:
  - Write an alert to Secure Flash Logs
  - Disable runtime access to detection engine functions

  - Block firmware reads or debugging until administrative override or wipe
  - Optionally, initiate self-deactivation mode if risk threshold exceeded

13.1.3.3 Facility-Level Physical Security (PE-3, PE-6)

- Critical facilities must:
  - Use badge-controlled access, mantraps, and CCTV retention (30 days minimum)
  - Maintain visitor logs and zone-based access control to sensitive zones (R&D, firmware signing labs)
  - Conduct quarterly physical access reviews and penetration testing

13.1.3.4 Tamper Incident Response

- Upon detection of physical compromise (device or facility), the following actions must be taken:
  - Escalate to Security Operations and Hardware Forensics Unit
  - Quarantine device(s) and log to the Hardware Compromise Register (HCR)
  - Notify Product Security Council and prepare report for incident board
  - Preserve any surveillance evidence, sensor data, or field logs
  - Replace affected hardware in field under secure RMA policy

13.1.3.5 Supply Chain & Transit Handling

- Shipments must include:
  - Tamper-evident seals on hardware and cartons
  - Serialization tracked end-to-end from factory to distributor
  - Carrier audit logs of custody transitions
  - Any breakage in chain of custody invalidates integrity unless reverified

13.1.4 Roles and responsibilities

- **Director of Firmware Engineering:** Oversees □ **Director of Hardware Security Engineering:** Oversees tamper design protocols and device-side detection response logic
- **Manufacturing Security Lead:** Ensures facility access control and shipment chain integrity
- **IT Security Officer (Facilities):** Manages access badges, surveillance, and zone-based enforcement

- **Incident Response Analyst:** Investigates tamper alerts and coordinates forensic evidence gathering
- **Compliance Officer:** Verifies alignment with NIST PE controls and supply chain regulations

13.1.5 Enforcement

Bypassing, disabling, or ignoring physical tamper events is a major security violation. All such cases will be treated as potential insider threat incidents. Violators will face immediate investigation, possible termination, and reporting to regulatory bodies if hardware compromise is confirmed.

13.1.6 Reference

- NIST SP 800-161: Supply Chain Risk Management for Federal Information Systems (PE-3, PE-6)
- ViraShield Device Security Architecture Blueprint (HW-SB-009)
- Hardware Compromise Register (HCR) SOP
- Secure Logistics & Chain-of-Custody Manual
- Secure Tamper Response Flowchart – Internal Field Manual

13.2 Vulnerability Management Policy

Frameworks: NIST SP 800-40, ISO/IEC 27001:2022 (Annex A.12 – Logging and Monitoring)

Policy #: VS-VMP-043

Policy Title: Vulnerability Management Policy

Policy Owner: Chief Information Security Officer (CISO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Risk Management, Threat Mitigation & Compliance

13.2.1 Purpose

To define the process for identifying, evaluating, prioritizing, and remediating vulnerabilities across all ViraShield systems—including firmware, cloud workloads, embedded devices, third-party libraries, and internal enterprise IT systems. This ensures timely protection against known weaknesses and aligns with secure development and operational resilience best practices.

13.2.2 Scope

This policy applies to:

- Firmware on ViraShield Portable AV devices
- Cloud services and supporting backend infrastructure
- Internal IT systems, developer endpoints, and CI/CD pipelines
- Open-source and third-party components used in ViraShield products
- All departments engaged in software development, infrastructure, and IT security

13.2.3 Policy Statement

13.2.3.1 Vulnerability Scanning & Inventory

- Weekly automated vulnerability scans must be performed on:
  - Production servers, endpoints, CI/CD containers
  - Firmware packages in staging environments
  - Open-source dependency packages (via SCA tools)
  - Results must be logged in the Vulnerability Inventory Register (VIR)

13.2.3.2 Severity Classification & Risk Ratings

- Vulnerabilities must be rated using CVSS v3.1 or newer:
  - Critical (9.0–10.0) → Remediate within 24–48 hours
  - High (7.0–8.9) → Patch within 5 business days
  - Medium (4.0–6.9) → Review and address in next release or maintenance cycle
  - Low (<4.0) → Monitor or address in backlog unless actively exploited
- Firmware-specific issues may also use embedded CVE scoring overlays

13.2.3.3 Patch & Remediation Protocol

- All validated vulnerabilities must follow a structured workflow:
  1. Triage → Confirm exploitability and affected systems
  2. Patch → Deploy hotfixes or OTA firmware updates
  3. Validate → Perform regression and exploit re-tests
  4. Close → Document resolution and update VIR status
- Vulnerabilities in third-party SDKs or libraries must be escalated to the Vendor Risk Management Lea

13.2.3.4 Threat Intelligence Integration

- The Security Operations Team must correlate vulnerabilities with:
  - Exploited-in-the-wild intelligence feeds

  - Known malware signatures and zero-day references
  - MITRE ATT&CK mappings (where relevant)
- Priority handling must be enforced for actively weaponized CVEs impacting AV signature logic or OTA pathways

13.2.3.5 Exception Handling & Temporary Risk Acceptance

- If a vulnerability cannot be patched within SLA, a risk exception form must be submitted to the CISO
- Temporary mitigations (e.g., network isolation, rule-based blocking) must be documented and implemented
- All exceptions must have a clear timeline and mitigation plan

13.2.4 Roles and responsibilities

- **Chief Information Security Officer (CISO):** Owns policy and monitors SLA adherence
- **Security Operations Center (SOC):** Performs continuous scans and intelligence monitoring
- **Firmware Engineering Lead:** Patches vulnerabilities in embedded platforms
- **Cloud DevOps Team:** Deploys updates and monitors CI/CD supply chain integrity
- **Vendor Risk Manager:** Coordinates external disclosures and remediations from third-party vendors
- **Compliance Officer:** Ensures alignment with ISO 27001 audit and documentation controls

13.2.5 Enforcement

Failure to patch or mitigate known high/critical vulnerabilities may lead to internal investigation, reporting to regulatory agencies, and disciplinary action. Willful neglect of remediation protocols may result in revocation of access privileges or termination.

13.2.6 Reference

- NIST SP 800-40 Rev. 3 – Guide to Enterprise Patch Management
- ISO/IEC 27001:2022 Annex A.12 – Logging, Alerting, and Remediation Controls
- OWASP Top 10 & CWE Mapping Index
- ViraShield Vulnerability Inventory Register (VIR) SOP
- Firmware Patch Pipeline & Validation Handbook
- CVSS v3.1 Scoring Calculator

- Risk Acceptance Form Template (SEC-FORM-RISK-002)

13.3 Insider Threat Prevention & Monitoring Policy

Frameworks: NIST SP 800-53 (AU-6, SI-4), ISO/IEC 27001:2022 (Annex A.7 – Human Resource Security)

Policy #: VS-ITPMP-044

Policy Title: Threat Prevention & Monitoring Policy

Policy Owner: Chief Information Security Officer (CISO)

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Human Risk Management & Threat Monitoring

13.3.1 Purpose

To detect, deter, and respond to insider threats across ViraShield's enterprise, including both malicious and unintentional internal actions that may compromise the confidentiality, integrity, or availability of systems, intellectual property, or customer data.

13.3.2 Scope

This policy applies to:

- All ViraShield employees, contractors, and third-party service providers with access to internal systems, development environments, or production infrastructure
- Systems involved in AV engine development, firmware R&D, cloud telemetry processing, and customer data retention
- Privileged access users across DevOps, threat intelligence, and licensing systems

13.3.3 Policy Statement

13.3.3.1 Insider Threat Definition

- Insider threats include any user who intentionally or unintentionally causes harm or facilitates unauthorized access, data leakage, system compromise, or service disruption due to misuse, negligence, or malicious intent.in the Signature Audit Log (SAL)

13.3.3.2 Behavioral Monitoring and Audit Logging

- Security Information and Event Management (SIEM) systems must:

  - Log access to source code, license validation keys, and firmware repositories
  - Monitor anomalous behaviors (e.g., bulk file access, off-hours data exports, unauthorized SSH usage)
  - Correlate user actions with baseline behavior profiles and risk scoring
- All admin and privileged user sessions must be recorded and retained for 180 days

13.3.3.3 Identity and Access Control Enforcement

- Role-based access controls (RBAC) and least-privilege principles must be enforced across:
  - Git repositories, OTA pipelines, AV detection models, production environments
  - Financial systems and customer data views
- Access reviews must be conducted quarterly and whenever personnel change roles

13.3.3.4 Detection & Threat Hunting Protocols

- Security teams must perform:
  - Insider threat hunting using behavioral analytics and machine learning
  - User activity reviews after any data loss, IP exfiltration, or system misconfiguration
  - Continuous monitoring for use of unauthorized USB drives, external email forwarding, or VPN tunneling

13.3.3.5 Reporting and Response Workflow

- Employees must report suspicious behavior using the Internal Threat Hotline (ITH) or the Secure Report Form
- The Insider Threat Response Unit (ITRU) must investigate within 24 hours
- Confirmed cases must be documented in the Insider Incident Register (IIR) and reported to the CISO and Legal Counsel
- If IP, AV code, or device telemetry was exposed, the Product Security Council must be notified

13.3.3.6 Awareness and Training

- All staff must complete annual Insider Threat Awareness Training

- Sensitive access holders (e.g., firmware, DevOps, threat intelligence) must undergo advanced detection training every 6 months

13.3.4 Roles and responsibilities

- **Chief Information Security Officer (CISO):** Oversees the insider threat program, approves response plans, and ensures integration with other enterprise risk management processes.
- **Security Operations Center (SOC) Manager:** Monitors audit logs, event data, and user activity across internal systems and cloud infrastructure to detect potential insider activity.
- **Insider Threat Response Unit (ITRU) Lead:** Coordinates investigations of insider-related incidents, manages evidence gathering, and liaises with legal and compliance teams.
- **Human Resources Manager:** Collaborates on disciplinary procedures and provides personnel records or behavioral history where necessary during investigations.
- **Department Managers:** Ensure team members are adhering to access control and acceptable use policies, and report any behavioral concerns or suspicious activity to the Security Operations Center.

13.3.5 Enforcement

Any employee or contractor found to have violated this policy through negligence or willful intent will face disciplinary action up to termination, legal prosecution, and permanent revocation of access credentials.

13.3.6 Reference

- NIST SP 800-53: AU-6 (Audit Review), SI-4 (System Monitoring)
- ISO/IEC 27001:2022 Annex A.7 – Human Resource Security
- Insider Threat Response SOP – INT-PROC-THRT-003
- ViraShield SIEM Analytics Rulebook
- Quarterly Access Review Checklist – ACCESS-AUDIT-007
- Insider Incident Register (IIR) Format & Review Protocol

13.4 Product-Specific Malware Incident Policy

Frameworks: NIST SP 800-61

Policy #: VS-PSMIP-044

Policy Title: Product-Specific Malware Incident Policy

Policy Owner: Director of Product Security

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Threat Response and Malware Containment

13.4.1 Purpose

The purpose of this policy is to establish a structured incident response process for malware-related events that originate from or affect ViraShield's Portable Antivirus device or its associated detection engines. This includes detection, analysis, containment, remediation, and continuous improvement based on malware trends affecting customer endpoints.

13.4.2 Scope

This policy applies to:

- Malware incidents detected or missed by ViraShield Portable Antivirus devices in the field
- False positives and false negatives identified through threat intelligence or customer reports
- Malware discovered during firmware validation, engine updates, or telemetry review
- Detection behavior issues related to specific platforms (Windows, Android, IoT)
- Security engineering, product security, threat intelligence, and customer support teams

13.4.3 Policy Statement

13.4.3.1 Malware Incident Detection and Escalation

- Any report of The Product Security Team shall follow the following response lifecycle adapted from NIST SP 800-61:
  1. **Preparation** – Maintain updated detection rules, behavioral indicators, and YARA signatures
  2. **Detection and Analysis** – Analyze host device logs, malware sample artifacts, and telemetry metadata
  3. **Containment** – Disable faulty signature distributions, suspend real-time scanning for affected engines if needed
  4. **Eradication** – Patch detection logic, remove malicious patterns, and validate updated engine behavior

5. **Recovery** – Push remediated definitions through over-the-air (OTA) update process or distribute offline patches
6. **Post-Incident Review –** Conduct root cause analysis, document lessons learned, and adjust engine heuristics

13.4.3.2 Zero-Day and Novel Threat Handling

- All zero-day malware samples must be handled by the Threat Intelligence Lab within 12 hours of confirmation
- If the sample bypasses behavior-based scanning, escalate to firmware engineering for model retraining
- If the malware modifies device drivers or cloud communication paths, notify the Incident Response Lead and activate emergency OTA quarantine rules

13.4.3.3 Customer-Facing Malware Event Reporting

- Customers affected by known malware events will receive:
  - A digital security advisory outlining symptoms, timeline, and mitigation
  - Access to the fixed signature or firmware via OTA update or offline patch tool
  - Option to submit additional samples or feedback through the Secure Feedback Portal

13.4.3.4 Coordination with External Entities

- ViraShield will coordinate with:
  - National CERTs (e.g., US-CERT, CERT-In) for widespread malware affecting multiple users
  - Cybersecurity Information Sharing groups to disclose variants and signatures
  - Third-party mobile or desktop vendors if a platform-specific rootkit or driver-level exploit is involved

13.4.4 Roles and responsibilities

- **Director of Product Security:** Oversees product-related malware response, ensures SLA compliance for incident handling
- **Threat Intelligence Analysts:** Analyze malware samples, update detection logic, and confirm false positives/negatives
- **Firmware Engineering Team:** Applies detection patches and behavior model updates across platforms

- **Incident Response Lead:** Activates broader security incident protocols if malware affects cloud infrastructure or license validation
- **Customer Support Team:** Notifies affected users, distributes updates, and triages incoming reports

13.4.5 Enforcement

Failure to respond to malware incidents in accordance with defined timelines or remediation standards will result in formal review by the Chief Information Security Officer and may trigger process audits. Unmitigated malware risks may also result in temporary suspension of OTA updates and external advisory release.

13.4.6 Reference

- NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide
- Malware Response SOP – Internal Reference: SEC-PROC-MAL-022
- OTA Signature Update Pipeline Manual
- ViraShield Threat Intelligence Telemetry Workflow
- Secure Feedback Portal Submission Policy
- Product Security Incident Severity Matrix – SEC-GUIDE-RESP-008

13.5 Portable Device Compatibility Assurance Policy

Frameworks: Internal Quality Assurance Standards

Policy #: VS-PDCAP-045

Policy Title: Portable Device Compatibility Assurance Policy

Policy Owner: Director of Quality Assurance

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: Internal – Product Quality and Platform Assurance

13.5.1 Purpose

To establish mandatory validation procedures and quality assurance controls that ensure the ViraShield Portable Antivirus device operates reliably and securely across all supported host platforms, including desktop, mobile, embedded, and consumer electronic environments.

13.5.2 Scope

This policy applies to:

- All operating systems and devices that interact with the ViraShield Portable Antivirus hardware
- Quality assurance teams, firmware developers, compatibility engineers, and support testers
- Supported platforms including Microsoft Windows, Linux, macOS, Android, Smart TVs, and vehicle infotainment systems

13.5.3 Policy Statement

13.5.3.1 Supported Platform Documentation

- A formal compatibility register must be maintained that includes:
- All approved operating systems and hardware configurations
- USB interface specifications (Type-A and Type-C)
- Power limitations, firmware response issues, and exception cases

13.5.3.2 Compatibility Testing and Certification

- All firmware builds and engine updates must undergo platform-wide validation across:
  - Windows 10/11, macOS (Monterey and newer), Ubuntu/Debian
  - Android versions 10–14
  - Smart TV OS: Tizen, WebOS, Android TV
  - Infotainment systems: Android Auto and embedded Linux
- Devices must successfully:
  - Enumerate on the USB bus
  - Initialize the antivirus engine
  - Detect baseline malware samples
  - Shutdown gracefully and securely upon removal

13.5.3.3 USB Interface Validation

- USB 2.0, USB 3.x, and USB On-The-Go functionality must be tested
- The device must reject non-compliant power levels or incompatible USB hosts without causing system instability
- Devices must default to secure fail-safe states if connection is not fully supported

13.5.3.4 Platform Issue Escalation and Remediation

- Platform-specific issues such as boot failures, firmware lockups, or scanning delays must be documented in the internal issue management system

- Critical platform issues must be triaged and patched within:
  - 3 business days (primary platforms)
  - 7 business days (secondary platforms)

13.5.3.5 Release Approval Requirements

- A formal compatibility certification report must be completed before releasing any firmware or engine update
- Releases without certification or QA sign-off are prohibited unless approved by both the Director of Quality Assurance and the Chief Information Security Officer

13.5.4 Roles and responsibilities

- **Director of Quality Assurance:** Oversees full compatibility test planning, certification scope, and final platform validation
- **Platform Compatibility Engineers:** Execute tests across host environments and document anomalies
- **Firmware Quality Analysts:** Confirm consistent scanning behavior and signature execution on all tested systems
- **Customer Support QA Leads:** Reproduce field issues and assist in compatibility documentation
- **Product Security Reviewers:** Ensure platform compatibility does not compromise AV performance or threat visibility

13.5.5 Enforcement

No firmware or engine release may proceed to production without compatibility verification across all supported host platforms. Non-compliance may result in rollback orders, security review, or formal release audits.

13.5.6 Reference

- Internal Compatibility Certification Checklist
- Firmware Platform Validation Manual
- Host Operating System Behavior Matrix
- USB Power Specification Compliance Sheet
- Smart Device Interaction Log (Annual QA Archive)
- Quality Escalation Protocol (QEP-04)

13.6 Regional Data Protection Policy (APAC)

Frameworks: Singapore PDPA, India DPDP 2023

Policy #: VS-RDPAPAC-046

Policy Title: Regional Data Protection Policy – APAC

Policy Owner: Chief Privacy Officer

Approval Date: March 29, 2025

Review Date: March 29, 2026

Policy Classification: External – Regional Data Compliance

13.6.1 Purpose

To ensure that the collection, processing, storage, and transfer of personal data by ViraShield Technologies Inc. in the Asia-Pacific region complies with national regulations, including Singapore's Personal Data Protection Act (PDPA) and India's Digital Personal Data Protection (DPDP) Act of 2023.

13.6.2 Scope

This policy applies to:

- All ViraShield operations, cloud systems, and customer interactions within Singapore, India, and surrounding Asia-Pacific jurisdictions
- Data originating from individuals residing in APAC countries where ViraShield operates or distributes products
- All employees, contractors, and regional partners handling data from APAC customers or systems

13.6.3 Policy Statement

13.6.3.1 Lawful Data Processing Requirements

- All data collected from individuals in Singapore or India must be processed only with lawful consent or a valid legal basis as defined in their respective data protection laws
- Data must only be used for the explicit purposes outlined at the time of collection

13.6.3.2 Consent Management

- ViraShield must obtain clear, informed, and affirmative consent before collecting or processing personal data
- Customers must have the ability to withdraw consent at any time via the ViraShield Privacy Preferences Portal

- Consent logs must be securely maintained for a minimum of five years for audit purposes

13.6.3.3 Cross-Border Data Transfer Controls

- Personal data collected from Singaporean and Indian citizens shall not be retained longer than necessary
- Data erasure requests from APAC users must be honored within 15 working days, barring legal or regulatory exceptions
- Data retention timelines must be defined and reviewed annually in the Regional Data Retention Matrix

13.6.3.4 Data Retention and Deletion

- All outbound data must be:
  - Anonymized before upload unless user is licensed and opted in
  - Limited to essential operational metadata (firmware version, threat hash, device type)
  - Regional upload nodes must be selected based on customer location and data sovereignty laws (e.g., GDPR, DPDP, PDPA)

13.6.3.5 Data Breach Notification

- Any personal data breach affecting APAC users must be reported to:
  - Singapore PDPC within 3 calendar days
  - India’s Data Protection Board within 72 hours
- Affected individuals must be notified without undue delay, with clear remediation steps provided

13.6.3.6 Vendor and Partner Compliance

- All regional vendors and data processors must sign a Data Protection Agreement (DPA) aligned with PDPA and DPDP standards
- Vendors must undergo annual privacy compliance audits and submit breach response plans

13.6.3.7 Regional Data Localization (India)

- Data categorized as “sensitive personal data” under the DPDP Act must be stored and processed within India unless exempted by the central government
- The Indian ViraShield data center must maintain strict access control, encryption, and logging in accordance with the DPDP compliance checklist

13.6.4 Roles and responsibilities

- **Chief Privacy Officer:** Ensures regional compliance, oversees cross-border data governance, and approves vendor data flows
- **Regional Compliance Officer (India/Singapore):** Monitors adherence to local privacy laws and coordinates breach response
- **Legal Counsel:** Reviews contracts, ensures lawful basis for all data processing, and maintains updated knowledge of regional legislative changes
- **Cloud Operations Manager:** Implements localization mandates and ensures secure regional data storage and encryption
- **Customer Support Manager – APAC:** Responds to individual rights requests and escalates data-related grievances to legal and privacy teams

13.6.5 Enforcement

Violations of this policy will result in disciplinary action and may trigger regulatory fines or service suspensions. ViraShield reserves the right to audit any system or third-party vendor involved in processing APAC-origin personal data.

13.6.6 Reference

- Singapore Personal Data Protection Act (PDPA)
- India Digital Personal Data Protection Act 2023 (DPDP)
- ViraShield Regional Data Transfer and Retention Guidelines
- Data Protection Agreement (DPA) Template – LEG-DOC-DPA-013
- Privacy Preferences and Consent Management SOP
- Regional Compliance Training Manual – APAC Edition

14 Appendix

14.1 Acronyms and Abbreviations

Abbreviation	**Full Form**
IAM	Identity and Access Management
NIST	National Institute of Standards and Technology
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
GDPR	General Data Protection Regulation (EU)
CCPA	California Consumer Privacy Act
HIPAA	Health Insurance Portability and Accountability Act (USA)
PCI DSS	Payment Card Industry Data Security Standard
SOC	Security Operations Center
OTA	Over-The-Air (Updates)
AI	Artificial Intelligence
ML	Machine Learning
AV	Antivirus
QA	Quality Assurance
APAC	Asia-Pacific
PDPA	Personal Data Protection Act (Singapore)
DPDP	Digital Personal Data Protection Act (India, 2023)
SSDF	Secure Software Development Framework
OWASP SAMM	Open Worldwide Application Security Project Software Assurance Maturity Model
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
CIS	Center for Internet Security
BCP	Business Continuity Plan
DPA	Data Protection Agreement

14.2 Referenced Frameworks and Standards

This section lists the regulatory and standards-based frameworks used to structure and implement ViraShield's security policies.

- **NIST SP 800-53**: Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-61**: Computer Security Incident Handling Guide
- **NIST SP 800-88**: Guidelines for Media Sanitization
- **NIST SP 800-213**: IoT Device Cybersecurity Guidance for the Federal Government
- **NIST SP 800-150**: Guide to Cyber Threat Information Sharing
- **NIST SP 800-147**: BIOS Protection Guidelines
- **NIST SP 800-40**: Guide to Enterprise Patch Management Planning
- **NIST SP 800-193**: Platform Firmware Resiliency Guidelines
- **ISO/IEC 27001:2022**: Information Security Management Systems (ISMS) Requirements
- **ISO/IEC 27017**: Guidelines for Cloud Service Information Security Controls
- **ISO/IEC 27701**: Privacy Information Management System (PIMS) Extension to ISO/IEC 27001
- **ISO/IEC 27034**: Application Security Framework
- **CERT Insider Threat Guide**: Best Practices for Preventing Insider Threats
- **PCI DSS v4.0**: Technical and operational requirements to protect cardholder data
- **GDPR & CCPA**: Data protection laws applicable to EU and California jurisdictions respectively
- **Singapore PDPA**: Personal Data Protection Act – Singapore
- **India DPDP Act 2023**: Digital Personal Data Protection Law – India
- **AMTSO**: Anti-Malware Testing Standards Organization Best Practices

14.3 Supplementary Organizational Artifacts

These internal resources were used or referenced in the construction of policies:

- ViraShield Risk Assessment and Impact Matrix – RISK-003
- ViraShield Privacy Consent SOP – PRIV-SOP-006
- Cloud Licensing Validation Protocol – LIC-CTL-001
- Incident Reporting & Escalation Flowchart – IR-DIAG-007
- QA Test Standard for USB AV Devices – QA-STD-USB-009
- AV Signature Expiry Timer Logic – DET-LG-021

14.4 Contact and Escalation Matrix

Internal departments responsible for managing, reviewing, and updating policies.

Role	**Responsibility Area**

CISO	Policy Oversight, Governance, and Enforcement
Chief Privacy Officer	Privacy, Data Protection, Regional Compliance
Director of IT / Cloud Ops	Infrastructure, Encryption, Network Resilience
Director of Product Security	AV Engine, Device Policies, Firmware Integrity
Head of Licensing & Subscriptions	Activation, License Verification, Deactivation
HR Director	Onboarding/Offboarding, Acceptable Use
QA Director	Testing Assurance, Device Compatibility

15 References

1) Anti-Malware Testing Standards Organization. (2018). *Testing protocol standard for the testing of anti-malware solutions (Version 1.0). https://www.amtso.org/wp-content/uploads/2018/05/AMTSO-Testing-Protocol-Standard-for-the-Testing-of-Anti-Malware-Solutions-v1.0.pdf*

2) California State Legislature. (2018). *California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100–1798.199). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5*

3) European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679*

4) Government of India. (2023). *Digital Personal Data Protection Act, 2023 (No. 22 of 2023). https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf*

5) International Organization for Standardization & International Electrotechnical Commission. (2011). *ISO/IEC 27034-1:2011 – Information technology — Security techniques — Application security — Part 1: Overview and concepts. https://www.iso.org/standard/44378.html*

6) International Organization for Standardization & International Electrotechnical Commission. (2015). *ISO/IEC 27017:2015 – Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. https://www.iso.org/standard/43757.html*

7) International Organization for Standardization & International Electrotechnical Commission. (2019). *ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. https://www.iso.org/standard/71670.html*

8) International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/standard/82875.html*

9) MITRE Corporation. (2023). *MITRE ATT&CK® framework.* https://attack.mitre.org

10) National Institute of Standards and Technology. (2012a). *Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2).* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

11) National Institute of Standards and Technology. (2012b). *Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1).* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

12) National Institute of Standards and Technology. (2014). *Guidelines for media sanitization (NIST Special Publication 800-88 Rev. 1).* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-88r1.pdf

13) National Institute of Standards and Technology. (2016). *Guide to cyber threat information sharing (NIST Special Publication 800-150). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf*

14) National Institute of Standards and Technology. (2018a). *Framework for improving critical infrastructure cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*

15) National Institute of Standards and Technology. (2018b). *Risk management framework for information systems and organizations (NIST Special Publication 800-37 Rev. 2). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf*

16) National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf*

17) National Institute of Standards and Technology. (2022). *Secure software development framework (SSDF) version 1.1 (NIST Special Publication 800-218). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf*

18) OWASP Foundation. (2020). *OWASP Software Assurance Maturity Model (Version 2.0). https://owaspsamm.org*

19) PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard (PCI DSS) version 4.0. https://www.pcisecuritystandards.org/document_library*

20) Republic of Singapore. (2012). *Personal Data Protection Act 2012 (No. 26 of 2012). https://sso.agc.gov.sg/Act/PDPA2012*

21) U.S. Congress. (1996). *Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf*

Document Owner: Chief Information Security Officer (CISO)
Approval Authority: Information Security Governance Board
Last Reviewed Date: April 1, 2025
Next Review Date: April 1, 2026
Version: 1.0

This policy document is reviewed and maintained by the Information Security Office of ViraShield Technologies Inc. Updates to this document shall occur annually or upon significant changes to organizational structure, infrastructure, compliance requirements, or threat landscape.

All modifications must be reviewed and approved by the Chief Information Security Officer and the designated Governance Board members.