# Information Security Management at VMware

This document contains descriptions and key elements of VMware information security policies.

vmware®

## VMware's Commitment to Information Security

Information security is important to VMware. VMware is committed to protect the integrity, confidentiality, and reliability of VMware information and information systems from unauthorized disclosure, removal, acquisition, modification, or destruction. VMware's information security service management and VMware information security policies are the foundation for the security of VMware information assets and VMware's obligation to its customers regarding information confidentiality, integrity, and availability.

## VMware's Information Security Organization

VMware has a designated Chief Security Officer to oversee information security for the enterprise. Multiple groups within VMware have a role in establishing, maintaining, monitoring, and operating security practices, including: Incident and Vulnerability Management, Security Operations, Information Security Governance, Risk and Compliance, Legal, and Internal Audit.

Service management has been established to ensure the right processes, technologies and service owners are in place to deliver, manage, and improve VMware information security services. VMware personnel have an obligation regarding the protection of information in accordance with VMware Information Security policies.

## About Information Security Policies @ VMware

VMware strives to achieve a high level of information protection standards. Relevant policies for information security have been established that are in line with VMware corporate objectives and in accordance with business requirements, relevant laws and regulations, contracts, and current or projected security threats.

Based on international standards ISO/IEC 27001 and consistent with industry-accepted practices and security frameworks, VMware information security policies define requirements for the protection of VMware information and information systems. These policies apply to all personnel who manage, use, or have access to VMware information assets, as well as to all VMware information assets and information processing environments including those infrastructures and services used to support VMware Cloud Services.

## Policy Oversight – VMware's Policy Executive Committee

All policies are required to have an Executive Owner who is a Vice President level or above. The Executive Owner approves the policy as well as any changes to the policy and ensures that the policy is reviewed and updated at least annually.

VMware's Policy Executive Committee has been established since 2016 to oversee new and significant changes to policies at VMware, as well as promoting compliance to those policies. Membership consists of twelve (12) executives (Vice President level or above) representing various business lines from across the company including Information Security, Legal, Compliance, Finance, Human Resources, and Internal Audit. At a minimum, this committee meets semi-annually.

## VMware Information Security Policies

Below lists and describes the policies implemented by VMware for establishing, implementing, maintaining, and continually improving information security.

VMware security practices are in line with many leading industry standards. The policies and practices referenced herein reflect a baseline standard and is intended to provide general confirmation of the implementation of such standards across the VMware business.

> ! Note: Specific policies implemented by VMware that are described herein are confidential and are not publicly available.

---

### Information Security Governance Policy

As the overarching policy, this policy governs information security at VMware starting with the company's commitment to information security. This policy defines the baseline for establishing an information security program, policies, and practices, as well as mandatory requirements for training and compliance. Roles and responsibilities are designated, and VMware's key information security principles are defined, including:

- Secure by design
- Defense in depth
- Least privilege
- Segregation of duties
- Risk and value-based security controls
- Control standardization and automation
- Auditability
- Independent review

### Acceptable Use Policy

This policy requires that information and information resources are used appropriately by VMware personnel. Monitoring of information systems is established where necessary for business purposes. Compliance with corporate policies is required for all users, including but not limited to VMware's "Statement of Policy on Equal Employment", "Prohibited Harassment Policy" and "Business Conduct Guidelines". VMware's core values include:

- Acting with integrity
- Avoiding conflicts of interest
- Complying with insider trading restrictions
- Respecting and protecting the personal information of others
- Complying with antitrust and competition laws
- Obtaining and handling trade secrets and confidential information of others with care
- Being mindful of trade control and anti-boycott laws
- Protecting confidential and proprietary VMware information
- Ensuring full, fair, accurate, timely, and understandable disclosure and financial reporting
- Complying with applicable laws and guidelines regarding records retention

### Security Incident Management Policy

VMware has established this policy to ensure the critical elements of the incident lifecycle are managed in a structured manner. The policy and associated procedures address the key elements of incident response, such as the handling, monitoring, and reporting of an information security incident, and forensics and remediation after an incident occurs, as relevant and applicable. Any suspicious or unusual activity must be reported to the incident response team. This policy and associated procedures align with the data breach requirements mandated by the global regulatory requirements of VMware office locations.

### Access Control Policy

This policy ensures system access and privileges to VMware information resources is managed to minimize risk, commensurate with the business need. System access is granted on a 'need-to-know' basis and for legitimate and authorized VMware-business needs. Segregation of duties is applied to privileges granted. Requirements are established for appropriate authorization, user access provisioning, change of access rights, access suspensions and terminations, inactive accounts, management of privileged access, and access revalidation.

### Authentication & Password Policy

VMware has established this policy to enable authentication mechanisms to protect access to VMware information assets. Key elements of this policy include the secure logon procedures, password configuration (complexity, restrictions for accounts, and testing), password administration, and user responsibilities for authentication (safeguarding authentication information and reporting compromised authentication).

### Encryption Policy

This policy provides VMware's encryption requirements to support the protection of information, covering both data-at-rest and data-in-motion. In addition to the required applications for encryption, key elements of the policy include encryption methods, secure cryptographic key management, and defined roles and responsibilities for maintaining compliance to essential cryptographic standards. VMware establishes cryptographic controls in alignment with relevant agreements, laws and regulations, including, restrictions on import/export of hardware or software with cryptographic capabilities, use of encryption to achieve information security objectives, and mandatory or discretionary methods of access. Cipher strengths in use at VMware are based on, at a minimum, industry standard practices.

### Business Continuity Policy

This policy governs VMware's corporate business continuity program. Requirements are specified to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence of, prepare for, respond to, and recover from disruptive incidents when they arise. Periodic business impact assessments drive business continuity plans for disaster events that would disrupt essential business operations, involve, or affect VMware personnel, office buildings or data centers, such as natural disasters, fires, floods, power disruptions, or any information security event compromising VMware's critical business services. This policy applies to all VMware users who manage or operate VMware systems or business services.

### Infrastructure Security Policy

In this policy, objectives for VMware infrastructure are defined in adherence to information security protocols designed to ensure that networks and associated applications and systems are managed and monitored in such a manner as to prohibit unauthorized access. This policy governs the maintenance, management, and ongoing improvement of network security practices. Controls are established for provisioning network connections, private network services, value added networks and managed network security solutions, such as firewalls and intrusion detection systems. Key elements of this policy include network controls, network configuration, and change management (segmentation, default deny, firewalls, audits), connections, IP address & subnet management responsibilities, and protocol policies.

### Production Control Policy

Under this policy, VMware implements restrictions on production environments such as requiring production be separated from both development and test environments. As well, standing permission to change, update, or add to production data is prohibited; production data can only be altered using formal change management processes. This policy confirms that production data is not to be used in test or development environments unless appropriate security measures are taken, such as data scrubbing, consistent with applicable law and contractual obligations.

### Change Management Policy

This policy ensures that a systematic framework is used for the documentation, testing and evaluation of all proposed changes to VMware's production environments. This policy ensures that mitigation of risks that could threaten stability, resiliency, security, regulatory compliance, and availability of VMware's production applications and infrastructure are addressed. This policy is applicable to all changes made to IT production environments. Key elements of this policy include requests for change, review and analysis, approval, communication, implementation (test, implement, post implementation review), fall back / roll back, and emergency changes.

### Backup Policy

To protect against loss of business-critical information and ensure continuous availability, this policy establishes data backup scheduling, testing, retention, and protection requirements for VMware production systems. Adequate backup accommodations are established to ensure that essential information and software can be recovered quickly following a disaster or media failure.

### Logging & Monitoring Policy

This policy establishes proactive measures to effectively log and monitor information system activities for the purposes of providing service assurance and preventing the exploitation of VMware information and information systems. Logging and monitoring help VMware to improve its security posture through the collection of system behavior. Log protection as well as controls around the logging and monitoring tools help to ensure the integrity of the data. Additional requirements include individual accountability, reconstruction of events, intrusion detection, and problem identification. This policy also provides guidelines for operational logs, error logs and security event logs that shall be maintained and reviewed for all critical operations and systems.

### Operations Security Policy

This policy ensures standardization of operational security throughout VMware's IT environment and ensures critical operating procedures are documented and maintained. Additionally, this policy provides requirements to ensure enterprise anti-malware software installation on development, domain, and production devices owned and operated by VMware which hold VMware information, passwords, or keys. VMware information is not to be stored on devices where anti-virus software is not maintained.

### Vulnerability Management Policy

This policy enables VMware to take measures for the discovery, evaluation, remediation, and management of vulnerabilities that affect VMware's information systems, information, or business processes. The policy applies to systems (devices, network devices, security devices) and applications (servers, database, custom and commercial applications) owned, managed, or operated by VMware. Key elements of this policy include identifying threats, vulnerability scanning and assessment, monitoring, patches (scheduling), reporting, and remediation.

### Asset Management Policy

Designed to ensure that company technology assets are identified, inventoried, and assigned a designated owner who has responsibility for its management and control over the asset lifecycle. This policy requires secure practices related to asset management including the return of assets, removal and security of any off-site assets, and secure disposal of assets.

### End User Device Security Policy

VMware has established this policy to minimize the risk of vulnerabilities presented when end user devices are used to access and use VMware information and information systems. Users are expected to ensure device security requirements (screen locks, passwords, anti-malware protection, encryption, idle-time passwords, and backups) outlined in this policy are followed. VMware has defined backup standards for staff devices that complement this policy. Other key elements of the policy include compliance requirements for all users, return of assets upon termination, mobile device management software, and maintenance and care of mobile devices.

### Data Classification Policy

This policy defines VMware's approach to data classification, and outlines responsibilities for ownership, labelling and secure handling. VMware implements secure data handling and protection standards at all stages of the data lifecycle (which includes data transmission, storage & disposal) to protect the confidentiality, integrity, and availability of data consistent with the assigned classification.

### System Acquisition, Development & Maintenance Policy

This policy requires that information security is incorporated across the lifecycle of information systems at VMware, including project management, system development, system enhancement, and system acquisition. Key elements in this policy include use of change control for deployment of information systems, restricted & secure access to program source code, use of open-source software, information security for new or enhanced systems, secure system engineering principles, outsourced development, and system security and acceptance testing. This policy is supplemented with Information Security Architecture Principles, Information Security Architecture Principles for Cloud, and Platform & Application Security Standards.

### Security Compliance Policy

This policy requires the identification of applicable legal, statutory, regulatory, and contractual requirements related to the security of information at VMware. Controls and individual responsibilities to meet these requirements are defined. This policy requires protection of corporate security records, and regular compliance reviews and audits of VMware information and information systems.

### Human Resources Information Security Policy

This policy is designed to ensure that the risks of personnel error, theft, fraud, and misuse are prevented or mitigated with appropriate hiring practices. The policy includes VMware's background screening practices upon hiring, requirements for the terms and conditions of employment, and required disciplinary processes for information security breaches.

### Physical Security Policy

This policy governs the safeguarding of offices, datacenters, support centers, and other business premises/ locations globally. It establishes the requirements necessary to physically secure VMware facilities, incorporating physical and environmental security measures to minimize risk, avoid threats, and eliminate vulnerabilities to protect information systems and staff. Key elements of this policy include perimeter security, physical entry controls, physical access controls, preventing misuse of facilities, protection against external and environmental threats, access to restricted areas, delivery and loading areas, supporting utilities, and clean desk/clear screen.

### Third Party Risk Management Policy

Ensuring the security of VMware information and information systems is not reduced when working with third parties, this policy establishes requirements for managing risk where third parties may have access to VMware's non-public information. Sourcing and business teams collaborate with information security risk to ensure a risk-based approach is taken with respect to all third parties to ensure the security of information assets. This policy defines the requirements for assessments to be performed as part of negotiating and reviewing third party agreements in line with VMware information security objectives and ongoing monitoring of such third parties for compliance. VMware vendors/suppliers do not have access to customer data/information unless required by a particular service offering.

---

This document is reviewed and approved by VMware Security & Resiliency.



**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com