

To Whom It May Concern:

VMware Inc. has established the following Information Security policies for the purposes of protecting the integrity, confidentiality, and reliability of VMware information and information systems from unauthorized disclosure, removal, acquisition, modification or destruction:

- Information Security Governance Policy
- Acceptable Use Policy
- Access Control Policy
- Asset Management Policy
- Authentication & Password Policy
- Back Up Policy
- Business Continuity Policy
- Change Management Policy
- Data Classification Policy
- End User Device Security Policy
- Encryption Policy
- Human Resources Information Security Policy
- Infrastructure Security Policy
- Logging & Monitoring Policy
- Operations Security Policy
- Physical Security Policy
- Production Control Policy
- Security Compliance Policy
- Security Incident Management Policy
- System Acquisition, Development & Maintenance Policy
- Third Party Risk Management Policy
- Vulnerability Management Policy
- Global Video Surveillance Policy

It should be noted that the VMware Security program and its associated Policies & Procedures are Proprietary and Confidential and therefore are not to be shared with outside entities. VMware information security policies were built in alignment with industry best practices / standards / frameworks such as NIST & ISO/IEC 27001, FIPS 140-2. Policies are reviewed on an annual and on an as-needed basis by the relevant stakeholders and revised as necessary. Policies are available for reference by all staff and contract resources and are hosted on the VMware Intranet.

Signed,

VMware Information Security Governance

