LAM INFORMATION SECURITY REQUIREMENTS FOR RECIPIENTS

Recipient must comply with this Information Security Requirements for Recipients ("InfoSec Requirements") for any Lam Information which it receives and retains.

"**Lam Information**" means: (a) all Lam Confidential Information (as defined in a contract, including Lam's Purchase Order terms, to which Recipient has agreed with Lam Research Corporation, its Affiliates, or any combination of them (collectively "**Lam**")); (b) all Personal Data, personal information, or other such similar term as may be defined under the EU General Data Protection Regulation ("**GDPR**"), the California Consumer Privacy Act of 2018, as amended, including by the California Privacy Rights Act of 2020 ("**CCPA**"), and other laws applicable to Lam or Recipient; and (c) all other data, records, files, information, in any form or format, accessed, received, stored, processed, or maintained by Recipient or its affiliates from or on behalf of Lam, including but not limited to technical information, even if anonymized.

"**Personal Data**" means an individual's first and last name when coupled with other personal information, including compensation, benefits, tax, marital/family status and other similar information about an individual, that Recipient may receive from Lam.

1. INFORMATION SECURITY POLICIES

Recipient must maintain a comprehensive information security policy framework that is aligned to industry standards, such as the NIST Cyber Security Framework, ISO27001, or their superseding or comparable standard. Recipient's policy framework must cover, at a minimum:

a. data classification, labeling, and handling;

b. acceptable use of information systems, including computing systems, networks, and messaging ("Information Systems");

c. information security incident management, including breach notification and procedures for collecting evidence;

d. host and network-based security controls, including anti-virus, an intrusion detection and prevention system ("IDS/IPS"), firewalls, and systems hardening requirements;

e. authentication requirements for end users, administrators, and systems;

f. access controls, including periodic reviews of access rights

g. logging and monitoring of Recipient 's production environment, including physical and logical access to Information Systems that process or store Lam Information; and

h. disciplinary measures for employees who fail to comply with such policies and procedures.

2. ORGANIZATION OF INFORMATION SECURITY

Recipient must maintain a technology and cybersecurity risk management program that is supported by an Information Security Officer ("**ISO**") and a dedicated team of security and technology risk professionals. Recipient must perform an annual risk assessment designed to identify, assess and manage risks to data and Information Systems.

3. HUMAN RESOURCE SECURITY

Recipient must require that its employees have a unique form of identification (e.g., badge), sign a non-disclosure agreement, and annually review and acknowledge Recipient's Code of Ethics and information security policies. Prior to employment, Recipient must perform a comprehensive background check that may include fingerprinting, criminal record, credit history, drug screening, and reference background checks, as permitted by law. Recipient must require that all employees complete annual information security training and must maintain a record of employees who completed such training. Additional security training based on role may also be provided.

4. ASSET MANAGEMENT

Recipient must implement policies and educate employees on how to appropriately classify, label, handle, and dispose of information and media based on the sensitivity of data. Recipient must:

a. maintain an asset inventory of Information Systems;

b. follow industry standards and applicable regulations when handling, processing and storing Lam Information both in on-premises and cloud environments; and,

c. implement procedures to sanitize or securely destroy media in accordance with current industry standards such as ISO 27001, SOC 2, and NIST 800-53.

For the use of personal mobile devices (e.g., Bring Your Own Device or BYOD) for work purposes, Recipient must enforce mobile device management controls consistent with industry standards including: (i) use of Mobile Device Management (MDM) software to ensure that Lam Information is appropriately contained, to control enrollment and revocation, and to ensure compliance with policies such as detection of jailbroken devices, weak passwords, unwanted applications, and operating systems that have not been updated, (ii) appropriate authentication and strong encryption controls, and (iii) ability to remotely wipe devices when necessary.

5. ACCESS CONTROL

Recipient must maintain identity and access management policies and controls reasonably designed to ensure that only authorized personnel are granted access to Lam Information. Recipient must track access requests and their authorization through a formal access management system. Recipient must (i) grant access based on the concepts of least privilege and separation of duties and (ii) limit access to those with a business need.

Recipient must:

a. Revoke access promptly following termination following internal transfer to a position where such access is no longer needed;

b. Assign unique identifiers to users that are traceable to an individual;

c. Review user accounts and their privileges on a regular basis, to verify that access is appropriate to job role, and remove access that is no longer required;

d. Restrict the use of privileged accounts to authorized employees performing system administration or security administration activities;

e. Collect, monitor, and retain access logs in accordance with industry standards;

f. Only use system accounts for system-to-system communication and configure them to prevent interactive logins from users; and,

g. Implement multi-factor authentication for access to Information Systems having Lam Information.

6. CRYPTOGRAPHY

Recipient must encrypt Lam Information during external transmission, physical transport, or authentication sessions, and while at rest on Information Systems. This includes tapes, removable media devices, laptops, network file transfers, and web transactions. Recipient must use encryption provided through commercial grade, industry-standard cryptographic algorithms (e.g., Advanced Encryption Standard (AES) 256, Transport Layer Security (TLS) 1.2), protocols, and key strengths. Recipient must manage encryption keys appropriately, including storage of keys in a separate location from the data they are encrypting and implementation of access controls that restrict access to keys.

Recipient must work with Lam to implement reliable and secure electronic data transfer methods that best satisfy Lam's requirements.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Recipient must maintain physical security measures to control and restrict physical access to Information Systems, including (i) cameras covering entry points into the secured data center and parking areas, (ii) intrusion detection and alerting capabilities, (iii) appropriate access control systems and logs, and (iv) infrastructure and environmental controls systems, including fire extinguishing, cooling, power and emergency systems consistent with local laws and industry standards.

8. OPERATIONS SECURITY

Recipient must maintain a reasonably appropriate security operations program designed to protect Lam Information and Information Systems that are tested and continuously improved. Recipient must maintain the following security controls as part of this program:

a. protection against data loss, malware, malicious intrusions and downloads;

b. updating anti-malware and antivirus signatures in a timely manner;

c. robust IDS/IPS;

d. monitoring for unauthorized access, connections, devices and software;

e. a security vulnerability program that includes monthly network vulnerability scans, timely patch management, and remediation of identified security vulnerabilities prioritized based on risk;

f. collection and correlation of security events from Information Systems and sensors to detect and address security events (i.e., Security Incident and Event Management or SIEM);

g. implementation of systems and devices using standardized, hardened builds;

h. monitoring and control of employee connections to the internet; and,

i. regularly backing up data as required to meet Recipient's continuity requirements and recovery time objectives in accordance with tested backup and restoration procedures, and protection of backups from loss, damage and unauthorized access.

9. COMMUNICATIONS & NETWORK SECURITY

Recipient must maintain reasonably appropriate network security and information transfer controls that are designed to ensure the protection of Information Systems, including firewalls, intrusion detection and prevention systems, antimalware, proxy servers and secure file transfer technologies.

Recipient must:

a. use multi-factor authentication for remote virtual private network (VPN) access and administration of specific core infrastructure components based upon risk, access to Information Systems having Lam Information,

b. leverage secure encryption technologies (e.g., Secure Shell (SSH), VPN, or TLS) for remote network administrative access (non-console);

c. implement a web-application firewall that checks traffic to detect and prevent web-based attacks against externally facing web applications;

d. implement a firewall between any demilitarized zone (DMZ) and Recipient's network;

e. implement a "deny-all" policy for firewalls except for traffic that is expressly permitted, test all firewall changes, and review firewall policies annually;

f. not store any Lam Information on systems connected directly to the internet; and

g. leverage industry standard protocols for encryption of external web application communications via HTTPS (e.g., TLS 1.2 or higher).

10. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Recipient must maintain a secure software development methodology that incorporates security throughout the development lifecycle, including application development policies, security training of application developers, and secure code reviews.

Recipient must do the following as part of its system acquisition, development and maintenance processes:

a. develop and configure applications and databases in a manner which is designed to protect the confidentiality, integrity, and availability of Lam Information;

b. develop web applications in accordance with security best practices (e.g., OWASP Top Ten), and reasonable steps to verify that web applications are configured to protect against the OWASP Top Ten vulnerabilities;

c. implement separate environments for production, development, and test;

d. conduct pre-release assessments or secure code reviews, including open-source reviews, and perform penetration testing of externally facing web applications used to provide the services, using automated scanning tools and manual analysis, on at least an annual basis, and ensure that identified vulnerabilities are remediated in accordance with documented policies that prioritize remediation based on risk;

e. upon request, provide an executive summary of latest penetration test conducted by an independent provider of Recipient's choice; and,

f. manage source code in accordance with documented procedures that restrict access and verify the integrity of code prior to deployment.

11. RECIPIENT RELATIONSHIPS

Recipient must maintain a vendor risk management program that includes regular evaluations of Recipient's suppliers that process Lam Information using a comprehensive risk/security assessment derived from Recipient security policies and industry standard practices.

Lam acknowledges Recipient may leverage cloud service providers in connection with the services provided to Lam. Recipient is responsible for the services performed by such services providers that process or store Lam Information to the same extent as if Recipient had performed the service itself. Recipient must have

written agreements with such service providers that are consistent with Recipient's information security obligations as applicable to the services performed by such service providers.

12. INFORMATION SECURITY INCIDENT MANAGEMENT

Recipient must maintain and regularly test its documented, comprehensive cyber incident response plan that is designed to identify potential threats, assess any risk exposure, report risks to management, and protect business operations. Recipient must do the at least the following as part of its information security incident management plan:

a. assess security events and suspected incidents;

b. respond by containing and mitigating incidents;

c. perform root cause analysis;

d. identify actions to minimize the risk of similar incidents from reoccurring; and,

e. conduct investigations in accordance with legal requirements for preserving evidence.

Recipient must promptly notify Lam at cybersecurity@lamresearch.com of any intrusion or compromise of an Information System that results in the access or acquisition of Lam Information by an unauthorized third party within 72 hours after becoming aware of such an occurrence (unless a different period of time is prescribed by a contract with Lam).