Information Security Standards for: Products hosted by AWS

Table of Contents

1. INFORMATION SECURITY POLICY

Flexera maintains a documented information security policy (the "Policy") to address the security, confidentiality and integrity of information provided in confidence to Flexera by its customers and partners. Flexera reviews its Policy at least annually to address changes in risks, technology and industry practices. Based on such reviews, Flexera may implement reasonable changes to the Policy.

2. INFORMATION SECURITY ORGANIZATION

INTERNAL ORGANIZATION

2.1 Flexera has an individual responsible for information security within its organization (the "Chief Information Security Officer") and has defined information security roles and responsibilities throughout the organization.

EXTERNAL PARTIES

2.2 Flexera has in place appropriate confidentiality protections with all contractors, subcontractors and other third parties who have access to Flexera's internal networks and/or will store, process or transmit Customer Classified Information ("Third Parties").

2.3 Flexera conducts assessments of Third Parties against these Information Security Standards before sharing Customer Classified Information with them.

2.4 Flexera includes appropriate security requirements in contracts with all Third Parties.

3. ASSET MANAGEMENT

3.1 Flexera maintains an inventory of its hardware and software assets that documents the identification, ownership, usage, location and configuration for each item.

3.2 Flexera maintains documentation and other records of baseline system and security configurations, including configuration changes for all hardware and software system components.

3.3 Flexera has formal policies and practices for performing risk assessments of software, systems and facilities. This includes classifying information and information systems, identifying security requirements, assessing and ensuring compliance with Flexera's policies and other applicable requirements and adhering to change management processes.

3.4 Flexera has processes in place requiring that its employees, contractors and other users abide by acceptable use and other policies, including these Information Security Standards.

4. HUMAN RESOURCES SECURITY

4.1 Flexera communicates to its employees, contractors and other internal users their responsibilities regarding information security and provides periodic refresher information security training Flexera enters into non-disclosure and/or confidentiality agreements with its employees, contractors and other internal users.

4.2 Flexera conducts background checks and/or other investigations as appropriate and permitted by applicable law, on all prospective employees.

4.3 Flexera's administrators are adequately trained on the Computing and Network Resources for which they are responsible.

4.4 Flexera promptly terminates access to Flexera's Computing and Network Resources and facilities and secure areas (e.g., data centers, telecommunications closets, etc.) when an individual leaves or discontinues work for Flexera, or no longer needs access.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

SECURE AREAS

5.1 Flexera has physical access control mechanisms (e.g., electronic access control, locks, etc.) to control physical access to Flexera Facilities.

5.2 Flexera locks and/or has access controls in place to control access to all of its data centers, equipment rooms, telecommunication closets and utilities.

5.3 Flexera controls unauthorized access to unattended areas (e.g., offices, conference rooms, etc.) within Flexera Facilities that contain Customer Classified Information by using locks or equivalent means.

5.4 Flexera Facilities and data centers are protected against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

5.5 Flexera personnel within Flexera Facilities (e.g., employees, visitors, resident contractors) are able to be identified (e.g., using identification badges, visual recognition or other means).

5.6 Flexera escorts visitors where Customer Classified Information or access to Flexera internal networks is readily accessible. Flexera data centers have a unique registry for all visitors and maintain access control logs.

5.7 Flexera controls delivery and loading areas and isolates these areas and storage areas from data centers, if possible, to avoid unauthorized access.

5.8 Flexera systems running on AWS are protected by Amazons physical security controls for more see. https://aws.amazon.com/compliance/data-center/controls/

EQUIPMENT SECURITY

5.9 Flexera has processes in place to protect its Systems, Network Devices and other equipment to reduce the risk from environmental threats and hazards and opportunities for unauthorized access.

5.10 Flexera has processes in place to protect its Systems and Network Devices used to process or store Customer Classified Information from theft, loss and unauthorized access.

5.11 Flexera has processes in place to protect equipment that is power-dependent from power failures, surges and other electrical anomalies.

5.12 Flexera has processes in place to protect power, telecommunication and network cabling from unauthorized access and damage.

5.13 Flexera maintains Computing and Network Resources and other equipment to enable its continued availability.

5.14 Flexera systems running in AWS are built to be fault tolerant across AWS availability zones.

6. COMMUNICATIONS AND OPERATIONS MANAGEMENT

OPERATIONAL PROCEDURES AND RESPONSIBILITIES

6.1 Flexera has standard operating procedures and supporting checklists in place for operational management of Systems, In-Scope Applications and Network Devices that address these Information Security Standards.

6.2 Flexera has a documented change management process and supporting procedures in place to control changes to Computing and Network Resources.

6.3 Flexera segregates duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of Flexera’s assets.

6.4 Flexera separates development, test and operational/production environments to reduce the risks of unauthorized access or changes to the operational system or information.

SYSTEM PLANNING AND ACCEPTANCE

6.5 Flexera has acceptance criteria for new Systems and Network Devices during development and prior to production release.

6.6 Flexera completes security configuration standards or “hardening documents” for all Server Systems, In-Scope Applications and Network Devices prior to placing them in production in accordance with these Information Security Standards and industry practices.

PROTECTION AGAINST MALICIOUS AND MOBILE CODE

Flexera maintains the following malicious software and mobile code controls:

6.7 Anti-malware software where commercially available is installed, configured, up to date and running on User Systems and Microsoft Windows Server Systems. The software is configured to protect against known threats, including, but not limited to viruses, worms, Trojans, rootkits, spyware and keystroke loggers.

6.8 Where the anti-malware software supports alerting, malware detections are automatically and promptly reported to personnel directly responsible for the infected device, who can address the alert and the root cause.

6.9 Upon detection of malicious software or content, the malware is promptly quarantined, blocked, disabled, confiscated or otherwise halted to prevent its spread. Detection and evidence gathering complies with all applicable laws and government regulations.

6.10 Devices are scanned at least weekly.

6.11 Anti-malware signature definition files are updated within 72 hours of release by the vendor for all Systems.

BACK-UP

Flexera has the following backup controls:

6.12 Data backups are performed prior to any system upgrade or maintenance activity.

6.13 Customer Information that is required to be encrypted in storage by these Information Security Standards remains encrypted throughout the data backup process.

6.14 Data backups are stored in a geographically separate, physically secure facility.

NETWORK SECURITY MANAGEMENT

Flexera has the following network security management controls:

6.15 A firewall is in place controlling access to Flexera networks. Firewall(s) define and enforce rules over information and users crossing between internal and external systems.

6.16 Firewall rules allow or deny connections based on business needs. Access which is not explicitly allowed is denied.

6.17 Flexera laptops, desktops and workstations have a software firewall installed and configured to block inbound traffic other than that required for business purposes and is not capable of being disabled, modified or updated by unauthorized personnel.

6.18 Connections between an external network (including, but not limited to the Internet) and Flexera's internal network employ intrusion detection (or prevention) capabilities. These capabilities (hereafter collectively referred to as “IDS/IPS”) may be included in firewall devices and/or by separate systems.

6.19 IDS/IPS systems are not disabled, update signatures used to identify malicious behavior no less frequently than every 60 days and provide alerts when significant events are identified.

6.20 Before changes are made to the perimeter of Flexera's network (e.g., a new Internet connection, adding a new physical site to the network, etc.), Flexera performs a risk assessment to confirm the change meets applicable policies (including, but not limited to these Information Security Standards).

MEDIA HANDLING

Flexera has the following media handling controls:

6.21 Flexera retains Information only for the purpose of, and as long as is necessary for, Flexera meeting its obligations to its customers.

6.22 Customer Classified Information stored on laptops is protected either through encryption or through physical protection against loss, theft and unauthorized access.

EXCHANGE OF INFORMATION

6.23 Flexera has policies, procedures and controls in place to protect the exchange of Customer Classified Information through the use of varying types of communication mechanisms.

6.24 Flexera encrypts Customer Classified Information when transmitted electronically, including wirelessly, over any network other than an internal Flexera network.

6.25 Flexera uses reliable transport or couriers when transporting physical media containing Customer Classified Information.

MONITORING

Flexera has the following controls for audit logging and monitoring:

6.26 Audit logging is enabled on Network Devices, Server Systems that contain Customer Classified Information, In-Scope Applications and all security-related systems and appliances (e.g., identity and access management systems, domain controllers, anti-malware management servers, etc.), where supported by the log source system, to capture security-related events.

6.27 Audit logs capture, at a minimum, the information for each security-related event defined below:

- User, system or process identifier that triggered the event
- Description of the event
- Date and time the event occurred (the date and time must be periodically synchronized to ensure it is accurate)
- Identifier of the system generating the event (e.g., IP address)
- Authorization information associated with the event

6.28 Audit logs are retained for not less than ninety (90) days.

6.29 Audit logs and/or error reports are reviewed regularly.

6.30 Audit logs subject to protocols intended to prevent accidental or intentional modification or destruction.

6.31 Applicable IDS/IPS events and alerts and other security alerts/events generated by other Computing and Network Resources, are handled according to Flexera's security incident monitoring, reporting and response process.

7. ACCESS CONTROL

BUSINESS REQUIREMENTS FOR ACCESS CONTROL

7.1 Flexera has an access control policy and limits authorized employees, contractors and other individual’s access to Flexera Facilities, secure areas (e.g., data centers, telecommunication closets, etc.) and Computing and Network Resources to only those individuals who are subject to appropriate confidentiality obligations and who have a legitimate need for access.

7.2 Access controls require positive identification and authentication of individuals.

USER ACCESS MANAGEMENT

Flexera uses the following user access management controls:

7.3 Privileges granted to an individual are the minimal set required for the performance of his or her job in a timely and efficient manner and only for the duration of the need.

7.4 Individuals are required to authenticate prior to the exercise of any elevated privileges (although the same identity and means of authentication may be used).

7.5 Passwords and PINs and other information used for authentication are encrypted.

7.6 Passwords and PINs are delivered in a confidential manner that requires the recipient to prove his/her identity before the password/PIN is received.

7.7 Passwords and PINs are not delivered in conjunction with their associated User ID via the same medium at the same time unless confidentiality of the delivery and proof of recipient identity is provided using industry standard public key cryptography.

7.8 Temporary, reset or initial passwords/PINs are unique for each individual and must be changed upon first use.

7.9 Proof of identification is provided and verified before a password or PIN is changed.

7.10 Default passwords/PINs are changed during or immediately upon the completion of the installation process.

7.11 Compromised accounts and accounts suspected of having been compromised are disabled within twenty-four (24) hours.

7.12 Upon an individual’s resignation or termination, the individual’s accounts are disabled and all shared passwords under that individual's control (e.g., service account password, etc.) are changed no later than seventy-two (72) hours after termination.

7.13 Flexera reviews access privileges regularly. Events such as changes in title or role trigger additional review and re-approval.

USER RESPONSIBILITIES

7.14 Flexera makes users aware of security requirements for selection and use of passwords and PINs and keeping them private.

7.15 Flexera trains or makes individuals aware to not leave Computing and Network Resources with an unlocked user interface unattended.

NETWORK ACCESS CONTROL

Flexera has the following network access controls:

7.16 Flexera limits access to Flexera’s network to only those employees, contractors and other users who have a legitimate need for access.

7.17 All remote access or wireless access communication sessions make use of network protocols that provide protection to all data in transport.

7.18 All remote access and wireless network services that grant unrestricted access to Flexera networks require the individual seeking services to be identified and authenticated before access is granted. Remote access to Flexera’s network employs two-factor authentication using a compliant password in combination with a one-time security code from a Flexera-approved service.

7.19 Direct diagnostic access to Flexera Systems or networks, for the purpose of monitoring or problem diagnosis and/or repair, does not allow elevated or administrator privilege without explicit enablement or access to any other location or service on Flexera's network.

7.20 No User System is connected to more than one network at the same time in such a way that it will route or bridge traffic from one network to another.

SYSTEMS, NETWORK DEVICES AND IN-SCOPE APPLICATION ACCESS CONTROL

Flexera uses the following access control mechanisms for all Systems, Network Devices and In-Scope Applications:

7.21 Access controls require positive identification and authentication of individuals.

7.22 Authorization decisions are based on an individual’s authenticated identity and the privileges granted to that individual.

7.23 User access privileges are disabled when no longer needed.

7.24 Individual passwords require a length of at least 8 characters and contain characters from at least 3 complexity classes (upper case, lower case, numerals and non-alphanumeric).

7.25 Individual passwords expire and must be changed every ninety (90) days. Passwords may not be reused for twenty-four (24) changes.

7.26 Ten (10) consecutive failed attempts to authenticate In-Scope Applications using a password within a thirty (30) minute period result in the account being locked or temporarily disabled for thirty (30) minutes.

7.27 Password authentication requires that passwords are not displayed to individuals in readable form.

7.28 Passwords are changed whenever there is any indication of password compromise.

MOBILE COMPUTING

Flexera has the following mobile computing controls:

7.29 User Systems are physically protected and require passwords.

7.30 A Mobile Computing Device is treated no differently than any other User System and encrypts confidential Information in transit.

7.31 Flexera is able to wipe information from Mobile Computing Devices (e.g., erasing the information or the encryption key protecting the information) upon a remote command. Remote wipe commands to erase Customer Classified Information are sent when the device is lost or stolen or upon detection that the security controls have been circumvented.

CLOUD COMPUTING

7.32 Access to Flexera cloud-based account follows the same controls as section USER ACCESS MANAGEMENT and SYSTEMS, NETWORK DEVICES AND IN-SCOPE APPLICATION ACCESS CONTROL.

8. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

CRYTOGRAPHIC CONTROLS

8.1 To the extent applicable, Flexera encrypts data in accordance with the table below using industry-standard algorithms and key lengths.

Process	Minimum Acceptable Encryption Method(s)	Data Type

Data transfer across any public network, including the Internet	IPSec or current version of TLS between hosts	All
Data transfer in email message body (i.e. non- bulk)	TLS transport layer encryption between email gateways where possible	All
Data storage on mobile devices and laptops	Whole Disk encryption or volume encryption employed	All

SECURITY OF SYSTEM FILES

Flexera has the following system security controls on Computing and Network Resources:

8.2 Software installations on Server Systems and Network Devices are evaluated in accordance with these Information Security Standards.

8.3 Software updates and patches are researched, tested and verified by appropriate Flexera personnel before installation.

SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

8.4 Flexera has a system development lifecycle for the development and deployment of Systems and In-Scope Applications, which incorporates activities and deliverables to address applicable security requirements.

8.5 Flexera does not use production data in non-customer-facing or non-production environments (e.g., development or test) unless the data is appropriately protected.

TECHNICAL VULNERABILITY MANAGEMENT

Flexera has the following technical vulnerability management controls:

8.6 Application and system owners regularly monitor applicable sources for information regarding security bulletins or the release of security patches from vendors.

8.7 Vendor-supplied critical security patches are applied as soon as practical, but no later than the periods set forth below:

- User Systems: within 30 days of vendor release.
- Internet-facing Server Systems: within 90 days of vendor release.
- All other Server Systems: within 90 days of vendor release.

Any exceptions to these time periods are reviewed, a risk assessment is performed, and the exception is documented.

8.8 Vendor-supplied non-critical security patches will be applied as soon as practical.

8.9 Flexera uses an industry standard vulnerability scanning tool to perform vulnerability scans of pre-production Internet-facing Server Systems and Network Devices prior to moving those Server Systems/Network Devices to production. Vulnerabilities identified in pre-production testing remediated prior to moving the Server System or Network Device to production on an as appropriate basis.

8.10 Flexera uses an industry standard vulnerability scanning tool to perform vulnerability scans of production Internet-facing Server Systems and Network Devices monthly. Vulnerabilities identified in production systems are remediated as soon as practical, but no later than the timeframes set forth above regarding critical security patches and non-critical security patches.

9. INFORMATION SECURITY INCIDENT MANAGEMENT

Flexera has formal security incident monitoring, reporting and response capability to identify, report and appropriately respond to known or suspected security incidents, including any unauthorized access, acquisition, use, disclosure or destruction of Customer Information. Flexera notifies applicable parties promptly of any known misuse of Customer Information.

10. BUSINESS CONTINUITY MANAGEMENT

10.1 Flexera has a business continuity plan ("BCP") aimed at assisting Flexera with a timely restoration of network and computing services in the event of system failure, damage or destruction.

10.2 Flexera tests the BCP no less frequently than once every two years.

11. COMPLIANCE

11.1 Flexera complies with known and relevant legal, contractual and regulatory requirements where applicable in its performance of its business.

11.2 Such compliance includes, but is not limited to the European Union's Global Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

12. DEFINITIONS

The definitions below contain a series of terms that are used throughout this document. When encountering one of these capitalized terms, refer to the definition below.

Computing and Network Resources: All Systems, In-Scope Applications, Network Devices and network services.
Customer: Any entity that provides information to Flexera for the purpose of furthering a contractual relationship between such entity and Flexera, including, but not limited to, customers and partners.
Flexera Facilities: Facilities which contain Customer Information.
In-Scope Applications: Applications, including databases and Internet-facing websites, that store, transmit or process Customer Classified Information, or Internet-facing websites that contain Customer public information.
Information Security Standards: The requirements described in this document.
Customer Affiliate: Any entity that controls, is controlled by or under common control with Customer.
Customer Classified Information: Customer and Customer Affiliate data, including Customer Personal Information, that, if disclosed to unauthorized parties, could result in a negative impact to Customer's or a Customer Affiliate's interests. Customer Classified Information will be reasonably identified as such.
Customer Information: Customer and/or Customer Affiliate data, including, but not limited to, Customer Classified Information, Customer Personal Information, or public information of Customer and Customer Affiliates that is provided to Flexera for hosting the information on a Flexera-hosted, Internet facing website or web application.
Customer Personal Information: Customer and Customer Affiliate data that identifies or can be used to identify an individual.
Mobile Computing Device: Handheld personal computing devices that can store information and communicate over wireless networks (including cellular and/or Wi-Fi), such as smart phones and tablets.
Network Devices: Systems and appliances that are part of the network infrastructure, such as routers, switches, firewalls, caching and proxy servers and load balancers.
Server Systems: Shared computer systems, including servers that provide file and print, collaboration, groupware, instant messaging, file transfer, application, or email services.
Systems: User Systems and Server Systems.
User Systems: Personal computing devices used by an end-user, including desktops, laptops, workstations and Mobile Computing Devices.

APPROVAL AND OWNERSHIP

Owner	Title	Date	Signature
Conal Gallagher	CISO	04/27/2022	Conal Gallagher
Jordan Hojati	AGC	5/9/2022	Jordan Hojati (May 9, 2022 10:14 CDT)

REVISION HISTORY

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	04/27/2022	04/27/2022	Conal Gallagher
1.1		5/12/2022	5/12/2022	Jordan Hojati
1.2		5/12/2022	5/12/2022	Marty Mellican