Quest Information Security Policy

Published on Jan/05/2024, version 1.3

This external policy is just a subset of the information that our internal teams adhere to. Should you have questions please reach out to the Account Executive that you are working with or send an email to security@quest.com

Scope

This policy applies to Quest Software Inc., One Identity LLC, and their Affiliates, all staff, consultants, contractors, and other third parties involved in computer-related activities associated with, where an Affiliate is any entity that directly or indirectly controls, is controlled by, or is under common control as Quest Software Inc. that develops, manufactures, markets, sells, promotes, or is involved in the general administrative aspects of the foregoing activities for products branded or sold under the “Quest” or “One Identity” umbrellas to customers other than the U.S. Federal Government.

It applies to all devices owned by Quest and its Affiliates or under their care or direction; used to store, transport, manipulate, and disseminate electronic data irrespective of how or whether they are connected to Quest’s and/or its Affiliates’ network(s). All departments and environments including Engineering, Development, and SaaS are included, as well as individuals and devices connected remotely or occasionally (such as laptops used by remote or traveling staff, US and non-US based consultants, Smartphones, etc.). Data in print or other forms such as on removable media is also covered by this policy. All employees, contractors, or other individuals using or having any level of responsibility for Quest-owned and/or its Affiliates-owned, -managed, or -used devices must comply.

If at any time you have questions about the appropriate use of a particular technology that is not covered in this Policy, you must exercise sound business and professional judgment and seek help from your management on any questions you may have.

Policy Statement

Quest Software Inc. (Quest) and affiliates takes security seriously for its employees, customers, suppliers and other engaged third parties. Quest and our associated affiliates, employees, suppliers, contractors and other third parties identified in this Quest Information Security Policy (Quest Associates) may access and use confidential information that belongs to employees and customers of Quest in order to deliver the products and perform the services we sell.

This policy (Information Security Policy) and its supporting standards and procedures have been developed based upon the industry standard ISO 27002 and corresponding NIST 800-171 which provides the foundation on which Quest develops and maintains a consistent and secure environment for the operation of its business processes. This Policy is based on administrative safeguards, technical safeguards and physical safeguards that together define and identify the responsibilities essential to the control of information security risk. Information is evaluated, classified and protected against unauthorized access, use, disclosure, modification and destruction. Security controls are intended to ensure confidentiality, integrity, availability, accountability, and auditability for important information and associated information technology resources.

The purpose of this Policy is to define baseline security controls and standards for the protection of Quest’s computer network(s) and information system resources (“System”). It covers both Quest and One Identity and is effective for all sites, portals or properties owned or managed by

either Quest or One Identity or associated with products designated with either a “powered by Quest” or “powered by One Identity” logo. References to Quest in this policy document should be read to include One Identity unless the context requires otherwise.

If you would like to view this Policy by country, please click here.

This Policy covers security requirements on all computer and network systems managed by Quest [or on Quest’s behalf] including network environments and online or web environments controlled, managed, owned or administered by Quest [or on Quest’s behalf] (“Quest Systems”) and any other storage method or material which may store and/or contain Quest-managed or Quest-owned information. The Policy also covers devices, including computing equipment (computers, servers, laptop computers and portable computing devices such as Smartphones, tablets and similar equipment) owned by or deployed by or on behalf of Quest (“Devices”). Any Device connected to a Quest System regardless of the ownership of that Device is governed by this Policy. No foreign, non-Quest-supported Device is permitted to be connected to any Quest System, without prior approval by the Quest Information Security (“IS”) or Information Technology (“IT”). This Policy also applies to any privately-owned Device connected to the Network or used to collect, process, use or store Quest data and information by any Quest Associates, whenever such Device is so used whether attached to and/or accessing Quest Systems as herein stated.

Compliance with Laws

Compliance with this Policy is mandatory for all Quest Associates as defined herein. Violations of this Policy or failure to comply with the standards or requirements laid out herein, whether deliberate or not, will be treated as serious misconduct. Quest’s design leaders have been assigned financial responsibility for information systems technology (including Devices) and associated information covered by this Policy and are held responsible for supplying necessary staffing and material resources to ensure proper compliance. Technology is continually changing, and Quest reserves the right to revise, modify, suspend, rescind, delete from, or add to this Policy from time to time in its sole and absolute discretion.

RELATED PROGRAMS AND POLICIES

Data Classification Policy

Quest’s Data Classification Policy is intended to work in coordination with this Policy to clarify roles, responsibilities and security strategies to the appropriate information used in or by Quest Systems and Devices in the appropriate way. It applies to all types of information, regardless of the form, including all paper or electronic documents, applications and databases, people's knowledge, and any other categorization of presentation of information relating to Quest is collected, used, processed, transferred or stored by Quest in its standard business operations. The Data Classification Policy also applies to all media types where Data, as defined in the Data Classification Policy, is stored.

Data and document owners determine the level of classification for data in their control in accordance with the five classifications listed above. More detailed information is referenced under the Data Classification Policy.

Asset Management Policy

Quest distributes devices and equipment owned by Quest to its employees as necessary and tracks asset and allocation data in order to maintain an up-to-date inventory of all information assets, computer equipment and software under its control. Server devices also have asset tracking software installed as a mandatory requirement. Configuration records identify external network connections to other systems, including firewalls, IP information, domain registrations and access ports (digital or analog). Owners are required to be identified for all Quest assets requesting access to Quest Systems. If no owner is found for any asset on the network, the asset is decommissioned. Ownership of all assets is to be clearly defined. This includes physical assets, electronic assets as well as data. All customer data ownership must also be identified contractually, and those records are required to be maintained and available for review in a secure centralized repository.

Quest manages a “bring your own device policy and process that requires password protection in accordance with Quest’s then-prevailing policy, the use of Quest managed cloud based data storage (only) with no files left on a local device or personal system, applying all security policies that may be applicable, such as locking the personal system when away from it, keeping system patches up to date and notifying the Internal Service Desk if the personal system is lost or stolen. Certain devices without adequate security profiles are strictly forbidden. Quest personnel are prohibited from using personally owned hardware and software on corporate information resources and hardware.

Media Handling Policy

Quest’s Information Technology team is responsible for establishing appropriate operating procedures to protect documents, computer media (USB Storage Drives), input/output data and system documentation from damage, theft or unauthorized access. Quest sensitive information may not be removed from Quest onsite business premises or storage and cloud services without proper approval from the designated Quest Data Owner. Quest data may not be stored in insecure locations or devices. Audit logs are maintained by the information owner or IT representative and made available to the Quest Information Security or Senior Leadership upon request. Use of removable media, including USB, Personal NAS and external drives is prohibited. Whenever any Quest owned, Quest leased, or Quest managed computer or network hardware is released from use, a full system image is required, or the hard drive is pulled and securely stored in a locked area. All software, Customer information and Quest information, whether sensitive or not, are made unrecoverable. All data is disposed of securely.

Information Security Management System (ISMS) Committee

The Quest Information Security Management System Committee is responsible for the review and approval of information security policy, standards, assessments, procedures, and other guidance developed by the Information Security. The Committee represents business, finance, legal, information security, human resources and leadership interests of Quest and provides a forum for the cross functional, identification and resolution of security issues, endorsement of security strategies, relevant risk and review of significant exceptions to information security policy.

ACCESS CONTROL

The Information Technology staff, and Quest Systems owner are both responsible for protecting the integrity of those Quest Systems and for configuring system security parameters consistent with this standard and all associated Information Security standards and procedures. Access to applications and data is granted to users only on a “need to know” basis, subject to approval by the designated owner(s) of the information assets.

User Account Management

Role-Based Access

Access to all Quest Systems is controlled by an owner-managed process which requires the system owner to obtain documentation of a justifiable business need to the information before allowing such access. All production business applications supporting material products or customers are secured by an access control system approved by Quest’s IS Team. Under this system, the information owner must approve any proposed access based on a business need-to-know associated with the requesting Associate’s role or job function.

Privileged System Access

The assignment of privileged system authority (e.g., the capability to use security administration commands, “superuser” status, local admin capability, and so on) for all systems is based on written justification only with annual re-justification required.

Review of User and System Access

System access and privileges are reviewed on an ongoing basis. Information System Owners are responsible for reviewing system access and privileges to ensure that they are revoked when no longer needed.

User Identification

Generic Accounts/Service Accounts

Generic and service accounts must have a defined and clearly published owners. These may not be used for interactive logon by anyone other than the account owner(s). All privileged service accounts and local administrative accounts are configured and managed by designated Quest IT resource(s). Privileged accounts must have a strong business case.

Contractor and Vendor accounts

All contractor and vendor accounts are uniquely identifiable and are recertified no less frequently than every ninety (90) days. Such accounts are required to have adequate background checks in place via Quest HR or via their contracted agency with approval by Legal and limited access based on time of day and the Quest Systems to which they connect wherever possible.

Sessions

Disconnected remote sessions related to Quest Systems and services are required to be configured so as to be reset in a timely manner given the application and resource in question, and forcibly reset upon account termination.

Login Failure Lockout

After ten (10) consecutive authentication failures, accounts are locked out of the resource impacted. Minimum lockout time periods will be subject to review by IS and the owner.

Password Protection

Quest follows the latest guidance from NIST on passwords. All passwords are enforced by the password granting system. Password construction qualities, such as duration, lock-out threshold length and age of the credential are required to be maintained by the Quest System in compliance with the ISP and relevant platform standard. Passwords and other access codes are kept confidential and changed following NIST 800-53 guidance. Passwords and access codes are required to be stored to memory or recorded using a secure mechanism (encrypted) that has been approved by IS.

Quest requires passwords of at least twelve (12) characters in length minimum, sixty-four (64) characters maximum. The previous 24 passwords should not be reused when technically possible to enable password history reuse limits.

Internet Security and Usage

Connections from Quest locations to the Internet are to be used for Quest sanctioned activities only, except as permitted under the “Acceptable Use of Technology Policy”. Quest Managed Service environments must have acceptable use parameters discussed with their customers.

Quest Associates are not permitted to transmit sensitive/confidential organizational information over the Internet unless encrypted to appropriate Information Security standards (listed in the Quest Cryptographic Policy. If such data must be transmitted, it is transmitted in an encrypted format, which is decipherable only by the intended recipient and only after it has reached a secure Quest System which is isolated from the Internet by a secure firewall.

Quest prohibits the granting of internet access from a Quest computing resource to persons other than Quest Associates. Connections from Quest to the internet prohibit all inward remote logins (such as device management) to corporate computer resources unless via one of the approved remote access solutions approved by IT and Information Security (IS) departments. All external remote access into a Quest computing resource requires use of two factor authentication, as well as the approval of the design and account management process via IS. Any external access or

use of PII information is required to be encrypted. Internet accessible services available are required to be segregated on separate devices within a DMZ or segregated network. Only web server-related functions are permitted on web servers. The use of anonymous file transfer protocol (FTP) must not be permitted on a web server but must rather be provided on a separate secure SFTP server configured for this purpose. Likewise, the web server must never be used as a domain name server (DNS). In both cases, vulnerabilities exist which could potentially damage both the website and the internal network. Management reserves the right to monitor all Internet connections to determine access levels and appropriate use of those connections, subject to local jurisdictions. Quest maintains software and systems that are capable of monitoring and recording activity to and from any computer Quest Associates may use.

Portable Computing Device Security Controls

For the purposes of this document the term “portable computing devices” refers to laptops, cell phones, tablets or other portable computing devices not classified as a desktop workstation or server class device. Portable computing devices must have consistent controls across the organization of their deployment. This implies a standardized and centralized issue and configuration point. Portable computing devices containing sensitive data must comply with Quest security and encryption requirements at all times. Connecting an unauthorized non-Quest managed personal computer device (e.g., desktop, laptop or wireless access point (WAP), tablet) directly to a Quest network is prohibited unless approved by Information Security. The unsanctioned use of devices capable capturing and or recording image or sound is prohibited unless it fulfills a valid business need and is approval by management and legal. Use of camera features should be available for any Quest business meetings or conference calls. The use of imaging and recording devices (e.g., Cell phone cameras) is generally prohibited, as is the use of personal network-attached storage devices to store company information.

TECHNICAL SAFEGUARDS

Documented operating procedures are required for critical business systems. The procedures are refreshed as needed (annually at a minimum). The storage of such procedural documents is centrally managed and securely backed up by each owner. The procedures are required to be readily available to those Quest associates whose job function requires the knowledge of said procedures. The granularity of these procedures is required to be at a level to allow for job rotation or assistance in the case of BCP or DR among operations personnel.

Network Security

External network connections among Quest Systems, including but not limited to links, wireless, gateways, switches, routers, protocol converters, are required to be designed and implemented in a manner compliant with the access control policies for each connected Quest System. As part of this assurance, all connections and changes must follow the Company’s change

management process and have documented approvals by Information Security prior to establishing new external connections.

All Quest network connections to non-trusted external networks (e.g., the Internet) are protected by a network firewall system which will ensure that only authorized users and information packets conduct business with Quest Systems. The level of filtering, supplemental authentication, audit logging, and associated access restrictions are based on a risk analysis of the Quest Systems and applications attached to both sides of the network connection.

Network segregation of Internet facing machines is required. Internet facing machines are placed within a DMZ that has been reviewed by Information Security and the IT team. Internal machines leveraging common back-office services do not require segregation unless those services are considered highly confidential (i.e. processing PCI data) or the ability to compromise internal production networks exist.

Wireless Access Points (WAP's) are installed by approved IT support staff. For wireless WAP's to allow access to an internal network, it is required to be reviewed by IS, configured with a VPN using strong encryption, and dual factor authentication (or SSO). For guest wireless access, the wireless WAP's must also be reviewed by IS and restrict access to internet browsing with sufficient acceptable use and URL restrictions.

The use of Quest owned hardware, software, or network elements to acquire, receive, store, or transmit files containing unauthorized copyrighted work is strictly prohibited. Any external network connections are documented, approved by Information Security and maintained and available in a rule set available for review upon request.

All Quest remote workers must adhere to Quest remote authentication policies. In summary, all sensitive information is encrypted on a portable computing device. In addition, two factor authentication is required to be in place for users to connect remotely into Quest networks. Remote workers are held responsible for ensuring that their workspace is a secure and private location in which they can protect the security of any Quest property required for their work, and any confidential information or intellectual property of Quest which is held in or accessible from their workspace. Any home office equipment such as routers, gateways etc. are required to be kept up to current security patch levels.

Encryption

Quest maintains a separate Cryptographic Policy to establish its policy framework for the use and deployment of encryption tools. Encryption tools approved by Quest IS and IT may be used to supplement physical and software access controls for protecting sensitive information on workstations, servers, and other computer systems. Where regulatory or customer mandates dictate encryption requirements, system owners must review with the business on specific

locations where encryption is required. Sensitive information must not be stored on local workstations, laptops or other portable electronic devices for more than 90 days and must always be encrypted.

Protection against Malicious and Mobile Code

Unauthorized devices must not be permitted onto the network or allowed access to internal Company resources unless they have been sufficiently secured. All devices allowed access to internal networks and facilities are required to be approved and managed systems in compliance with security and IT requirements. Disabling malicious software protection at the server or laptop level is strictly prohibited. An approved malicious software protection product are required to be installed and active before the device is placed in use and it must remain installed and active until the device is taken out of service. Malicious software protection products must not be turned off without the written approval of IS.

All systems are required to be configured to receive malicious software definition file updates daily. Testing by IT prior to delivery are required to be completed. High priority critical updates are required to be tested and implemented immediately. All Systems need to have EDR (Endpoint Detection and Response) capabilities and Quest's endpoint management tool installed.

Authorized devices must allow management and support by IT staff to the requirement level mandated within this Policy. Contractors must use managed Quest computers when working within internal network and facility locations or have approved security software or approval from management.

All workstations are equipped with software for detecting the presence of malicious software. All new software is required to be properly screened (i.e., scanned) with malicious software protection tools approved by IS before being used on laptops and file servers. If authorized mobile code is executed, all company controls and standards are required to be in place to ensure proper execution of code.

Software Security Requirements

Certain types of applications, such as those used for messaging, remote access, encryption, and system security, are required to be approved by Quest IT and IS prior to use or implementation in any Company network or system. Quest maintains an official list of approved software applications. The installation and use of any personal software without approval of Quest IT and IS is prohibited. Prior to use by Quest Associates, all data, software, storage media, and pre-configured systems obtained from sources external to Quest are properly screened and/or quarantined to reduce the likelihood of contamination by malicious software.

Change Management and Monitoring

Quest maintains industry-standard process and requirements relating to both Quest System or policy change management on ongoing monitoring of the Quest System environment. Every change to a critical Quest information asset resource, such as operating system, computing

hardware, network, and application is subject to the change management policy and must follow change management procedures.

Segregation of Duties

Developers are prohibited from maintaining regular access customer production systems. Developers must inform and obtain approval from the system owner(s) before accessing or modifying production environments. Notification of access and changes to customer production products and segregation requirements are part of the product Software Development Life Cycle (SDLC) and include all customer requirements.

PHYSICAL AND ENVIRONMENTAL SAFEGUARDS

Adequate security measures are in place to protect the Quest facilities as well as computer and communications equipment and data from physical damage, theft, power surges, electrostatic discharge, magnetic fields, water, overheating, and other forms of physical threats.

Physical Entry Controls

Physical access to all data assets and computing facilities, such as data centers or server rooms, is documented and managed. All Quest staff, contractors, vendors, customers, and visitors must display a Quest issued identification badge while in any Quest facility. Requests for access must come from the applicable Quest System owner. Once granted, access cards, fobs and/or keys must not be shared or loaned to others. Access cards, fobs and/or keys that are no longer required are immediately returned to the person responsible for the computing resources and or the restricted facility. Cards must not be reallocated to another individual bypassing the return process. Lost or stolen access cards, fobs and/or keys are reported to the person responsible for the computing resources and or the restricted facility. Cards, fobs and/or keys must not have site address identifying information (e.g., facility information), subject to local jurisdictions, other than a return mail address.

All Quest Systems, resources and or restricted facilities that allow access to visitors must track visitor access with a sign-in/out log. Card or fob access records and visitor logs for computing resources and or restricted facilities are kept for routine review based upon the criticality of the computing resources and or what is being protected. Visitors should be escorted at all times by a Quest Associate that will be accountable for their actions.

The process for granting card, fob and/or key access to computing resources in restricted facilities for a third-party non-Quest Associate must include the approval of the person responsible for the facility in addition to background checks. Third party non-Quest Associates that are granted access rights to a Quest System or resource in a restricted facility may be required to receive emergency procedure training for the facility and must sign the appropriate access and non-disclosure agreements.

Maintenance logs for repairs and modifications to physical components (hardware, walls, doors and locks) and for repairs and modifications to physical components of a facility are maintained.

Equipment Security

All multi-user information systems equipment (e.g., servers, routers, firewalls, switches) are stored in limited access rooms and/or be otherwise protected from tampering or other forms of unauthorized physical access. Media that contains confidential and restricted materials, (e.g., PII), are encrypted and/or transported in locked containers. Any third party suppliers must have rigorous security controls that have been reviewed by the Quest business owner along with Information Security. Suppliers handing material must have been additionally reviewed by Legal for sufficient legal contract language.

SECURITY INCIDENT RESPONSE

All Quest personnel, business associates and third parties who observe (or suspect) security weaknesses, vulnerabilities (or potential threats) are required to report them to their IT Systems Administrator and Quest Information Security immediately at security@quest.com.

The Security Incident Response Policy and Procedure establishes the rules for dealing with actual and suspected computer security incidents. Security incidents include but are not limited to: malicious software and unauthorized use of computer accounts and Quest Systems. All Information Security incidents are reported without delay to Quest Cybersecurity for prompt identification of any penetration achieved, damage caused, restoration and repair, and to facilitate the gathering of any associated evidence. Each department maintains a helpdesk process for users to report information security issues, such as potential threats, observations, suggestions and incidents. Appropriate personnel investigate reports.

Once a security incident has been reported, the Information Security Team reports the incident to Quest Legal for guidance concerning customer notification. Following legal guidance and following the guidelines of contacting the media (if applicable), the details of the incident, its status, and actions taken by Quest to deal with the incident is reported to the customer or individuals as necessary. Quest applies a “lessons learned” methodology as an integral part of the Security Incident Response Policy and Procedure. Business management reviews material security incidents at the quarterly ISMS meetings to form a continual maintenance and improvement strategy.

Security in Third Party Agreements

All third-party outsourced contract agreements include an obligation to provide robust protection to Quest Systems and network environments as well as Quest’s customer confidential information. These contracts require the outsourcer to maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the confidential and sensitive electronic information to which it has access on behalf of Quest. Outsourcing service providers are required to protect against any anticipated threats

or hazards to the security or integrity of such information that could result in substantial harm or inconvenience to Quest or its customers.

Thorough due diligence is conducted before selecting a third-party business associate who will have access to Quest sensitive information, including customer information or Quest operating facilities. Important elements of due diligence in selecting a third-party business associates include financial stability, business strategies and goals, human resources policies, service philosophies, quality initiatives, and cost management policies. Consideration must also be given to the third party's culture, values, and business styles and how likely they will fit with Quest's culture

The security requirements stipulated in the contractual agreement between Quest and the third-party business associate are regularly reviewed between the third party and Quest during the entire term of the contract.

Evaluation criteria will include account termination provisions if it is determined upon review of the contract that the third-party business associate has violated a material term of the contract concerning information security. A proper risk assessment is done on all vendors that have access to Quest confidential information.

Business Continuity Planning (BCP)

Adequate plans and procedures must exist for the backup of critical computer and network resources and for the prompt recovery of services following unanticipated interruptions. The feasibility of BCP Plans is subject to annual review, completed by either conducting a walk-through and/or testing of any or all of its parts.

PERSONNEL AND HUMAN RESOURCES SECURITY

All Quest Associates with access to Quest Systems must have adequate background screening processes in place (through Quest or an approved contractor). The background check screening process includes criminal checks, regulatory and employment history verification checks in accordance or to the level allowed by local jurisdictions.

Quest is committed to providing regular and relevant information security awareness communications to all staff by various means, such as electronic updates, briefings, newsletters, etc. Information and policies relating to information security are maintained on the Quest intranet site Policy Central which is available to the entire Quest user population.

Quest managers are responsible for providing prompt notification to HR for the Quest Associate status changes (e.g., terminations or transfers). The HR personnel must immediately notify IT staff to suspend, cancel, and/or adjust all access privileges associated with changes in status of such users.

Human Resources organizations are responsible for timely notification to IT of all changes in employee status affecting information system access privileges.

Managers of departments within Quest involved with contractual arrangements that permit access to Quest Systems by non-Quest entities are responsible for notifying the appropriate IT, Legal and Quest Information Security of contractual changes affecting access privileges granted to the non-Quest entity.

The Quest System owner (custodian) is the individual at Quest responsible for the IT management of the Quest System access. Each such data system owner must implement and maintain periodic follow-up review and corrective action procedures to ensure timely adjustment of access privileges associated with transfers, terminations, and changes in contractual agreements with non-Quest entities.

Site facility personnel are responsible removing any card and/or key fob access rights of individuals that change roles within Quest or are separated from their relationship with Quest. Access revocation occurs immediately upon notification of involuntary termination of employment or be timed with the date of the planned or voluntary termination date.

This external policy is just a subset of the information that our internal teams adhere to. Should you have questions please reach out to the Account Executive that you are working with or send an email to security@quest.com

Document Control

Version / Status	1.3	Published
Review Frequency	Annually	
Last Review Date	01/05/2024	
Next Review Date	01/05/2025	

Approval-2024-01-05.pdf