Data Breach Response Policy

Quest Software Inc. and One Identity LLC are focused on the development of high value software products designed to optimize, organize, manage and protect data and systems on a variety of platforms and environments. Technical support and consulting services are also provided in connection with those products.

As providers of cloud and on-premises software products, Quest and One Identity each take the security and confidentiality of our customers' information very seriously. We are committed to maintaining and improving our information security practices and minimizing our exposure to security risks.

Purpose

Our intentions for publishing this Data Breach Response Policy are to focus attention on data security and potential breaches of that security and to show how our established culture of openness, trust and integrity should help us to respond when potential breaches occur. We are committed to protecting our customers, employees and partners from illegal or damaging actions by individuals, companies or rogue organizations, whether or not those actions are intentional.

This Policy describes the procedures and safeguards employed by Quest and One Identity whenever there is a threat of a data breach or other incursion on data collected, stored, processed or managed by either of us ("Breach"). We take this approach for data we hold, manage or process for ourselves and our employees, but we also do this on behalf of our customers. This Policy also describes the actions that will be taken based on the type and severity of the Breach and those necessary to remediate a potential Breach.

Scope

This Policy applies to all team members of both Quest and One Identity (including all employees of any affiliate of either), all "non-employee" assigned workers performing services for or at one of our facilities (e.g., consultants, independent contractors, outsource service providers, general services suppliers, vendor funded personnel, and assigned worker/agency temporary workers), and any other third parties doing business with or acting directly or indirectly on behalf of Quest or One Identity. Compliance with this Policy is mandatory for you and is a condition of your employment, assignment or engagement with one of us. This Policy is intended to describe the measures each of Quest and One Identity will take to comply with (among other things) the European Union's General Data Protection Regulation ("GDPR") and the U.S. National Institute of Standards and Technology Framework (the "Cybersecurity Framework") for Improving Critical Infrastructure Cybersecurity (together, the "Privacy and Cybersecurity Laws").

Reporting a Potential Breach

Any time you suspect that a theft, Breach or exposure of Protected Data or Sensitive Data (as defined in the Privacy and Cybersecurity Laws) may have occurred, you should immediately report a description of the potential theft, Breach or exposure to Quest's or One Identity's Legal Counsel at DPP@Quest.com or by calling 1-800-603-2869, or in person. International hotline numbers can be found here. All reports of potential theft, data Breach or exposure will be investigated to confirm if a theft, Breach or exposure has occurred. If a theft breach or exposure has occurred Quest's or One Identity's SIRT (Security Incident Response Team) , as appropriate, will follow its own requirements for response and remediation of potential breach situations. These requirements are outlined in detail in Quest's and One Identity's internal breach response procedures as part of the Quest and One Identity Incident Response Policy.

Confirmed Breach of Provider's Protected or Sensitive Data

As soon as a theft, data breach or exposure containing Protected Data or Sensitive Data is identified, the process of removing all access to any compromised resource will begin. An internal SIRT will conduct a comprehensive incident response. The internal response team includes representatives from:

- Information Systems
- Information Security
- Business Operations
- Legal
- Corporate Communications
- Human Resources
- Business Management

This internal team will perform data forensics to analyze the incident to determine the root cause; the types of data involved; the number of internal/external individuals and/or organizations impacted.

Responding to a Breach

When a response is required, the Quest or One Identity SIRT, as appropriate, will be responsible for defining a response communication plan in accordance with regulatory requirements as defined in the GDPR of potentially disclosed data and the requirements of the individual case. The communication plan may include notification to third parties, regulators, law enforcement or any other party and will be determined with the direct advice and guidance of the respective Legal and Compliance Team.

Remediation of a Breach

In parallel with investigative and notification response measures, actions may be taken to introduce the necessary safeguards to remediate any vulnerabilities and concerns described in the investigative forensic report. Remediation measures may include any or all of the following:

- Arresting any additional data loss
- Review and refinement of incident avoidance and data breach policies
- Remove improperly posted information from the web
- Secure all websites
- Assess third party service providers access privileges
- Develop forensic review plan/review network segment exposure
- Awareness Training

Again, Quest and One Identity take the confidentiality, integrity and availability of their customers' information very seriously. We are committed to maintaining and improving our information security practices and minimizing exposure to security risks. To ensure currency and ongoing relevance, this policy will be reviewed at least annually and updated accordingly.