Security Policy

Qvest.io

Effective date: September 4th, 2020
Approved:

Niels Søholm
CTO & Security Administrator

Introduction

This Security Policy is a formal set of rules by which those people who are given access to company (Qvest) technology and information assets must abide. The main purpose is to inform company users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the company. All employees are expected to have knowledge of these policies and are required to report violations to the security administrator.

Classification of data

Data can have different values. Gradations in the value index may impose separation and specific handling procedures for each kind. The data classification levels listed here are referenced in the following sections.

#	Name	Description	Example
1	Sensitive production data	Personal data of users	Email address of a Qvest participant
2	Restricted production data	All other data stored and processed in Qvest product	Topic of a Qvest
3	Customer relation management data	Data generated and used in sales and support efforts	Support email correspondence
4	Internal data	Non-customer private data	Qvest strategy document
5	Public data	The remainder	Approved customer testimonial

Risks

The main risks that motivate these policies are public exposure of private data and loss of important data belonging to Qvest and its customers.

Broadly speaking there are three types of actors who pose a threat:

1. **Employees -** Qvest's own employees may do damage through incompetence or on purpose. They may expose or lose data.
2. **Amateur Hackers and Vandals -** The most common type of attackers. These amateur hackers are scanning and looking for well known security holes that have not been plugged. They may attempt to trick employees to give up access or data through scam mail and websites.

3. **Criminal Hackers and Saboteurs -** The probability of this type of attack is low. The skill of these attackers is medium to high. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

By adhering to the policies of this document employees at Qvest contribute to mitigating the internal vulnerabilities and protect against malicious external actors.

User classification and authorization

The company has established the following user groups and defined the access privileges (authorization):

Category	**Access privileges**
Security administrator	Full access to all systems.
System analyst/developer	Access to systems with data at classification level 3-5. Access may be elevated to systems at classification level 1-2 on a case-by-case basis, if needed for certain tasks. The security administrator grants this elevated access.
Qvest employees* and contractors**	Access to systems required for job functions. Generally includes systems with data at classification level 3-5 and in case-by-case basis may include level 2. The security administrator grants this elevated access.
Customers	Full access to data stored by their users at their organization in the Qvest product. The product imposes further authorization levels among users at the customer.
General Public	Access to systems exposing data at classification level 5 only.

*Qvest employees (e.g. support staff) may request temporary access to a given customer's data (classification level 1-5). Certain users (admins) at the customer have authorization to grant such access and revoke it at any point.
**Contractor access to company information and systems must be approved by the company CEO.

Policies

List of security policies:

- **Access Control**
  All users will be required to present a unique ID (e.g. email address) and password to

access company systems. Users must comply with the following rules regarding the creation and maintenance of passwords:

- must not be found in any Danish, English or foreign dictionary.
- must never be written down physically
- must not be reused across multiple accounts/systems
- must never be shared with anyone

Access to systems that store or process data at classification level 1-2 (see table above) requires 2-factor authentication in addition to ID and password.

- **Local network**
  Only authorized devices may be connected to the main local network (Qvest). Authorized devices include laptops, workstations, smartphones and storage devices owned by the company that comply with the configuration guidelines of the company. A guest network (Qvest-Guest) is in place which may be used for personal devices and devices of visitors. Visitors may never connect to the main network. Employees may never connect storage devices from visitors to company devices.

- **Remote Access**
  Only authorized persons may remotely access the company network. To access the company network and any company systems containing data at classification level 1-2 (see table above) via a remote network an approved VPN connection must always be used.

- **Monitoring**
  The company has the right to monitor electronic information created and/or communicated by employees accessing systems processing data at classification level 1-4 (see table above).

- **Acceptable use**
  User accounts on company devices are to be used only for business of the company and not to be used for personal activities.

- **Data retention**
  Personal data is stored for no longer than is necessary for the purposes for which the personal data is collected and processed. Qvest systems automate deletion of data at classification level 1 within 4 months of last known usage. It is the responsibility of Qvest employees to ensure any additional customer or employee data that has no further use is deleted.

Incident handling procedure

The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network. Some examples of security incidents are:

1. Illegal access of a company computer system.
2. Damage to a company computer system or network caused by illegal access.
3. Denial of service attack against a company web server.
4. Malicious use of system resources to launch an attack against other computers outside of the company network.

Employees, who believe their devices or Qvest systems have been subjected to a security incident, or have otherwise been improperly accessed or used, should report the situation to the security administrator immediately.

Security Administrator

At the time of writing the security administrator role is fulfilled by:

Niels Søholm
+45 29 25 45 85
niels@qvest.io

In the event that the role is reassigned, this will be announced internally and a new revision of this document will be made available.