



Qalixa Security Policy

Prince & Queen AB

Göteborg, Sweden, 2009

1 General

- 1.1 There are several objectives of a security program, but the main three principles here are preservation of availability, integrity and confidentiality of customer specific information and data. These objectives and/or statements are enforced by a set of applied Control Instruments

2 Physical security

- 2.1 Statement. Critical or sensitive information processing facilities shall be housed in secure areas protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.
- 2.2 Control Instruments. QALIXA infrastructure is hosted in Scandinavian Hosting hosting centre in Stockholm, Sweden. While QALIXA manages hardware and software, the hosting centre provides services like electricity, cooling, physical security, shipments etc. This centre provide global enterprises, content companies and network service providers the most secure, fault-tolerant, redundant, flexible and cost-effective Internet infrastructure solutions in the industry.

3 Network Access Control

- 3.1 Statement. Unauthorized access to network services shall be prevented and user access to both internal and external network services must not compromise the security of the services.
- 3.2 Control Instruments. Seller A firewall separates the QALIXA corporate network from QALIXA production environment. Therefore, unauthorized employees cannot access data from the corporate network infrastructure. Access is limited to specific roles or functions within QALIXA. Additionally, access is managed on an "exception" basis whereby personnel need clearance to be authorized. Access is time-limited, after which time reauthentication is required. The access lists are administrated using a dedicated access control product which is integrated with the firewall equipment. Another firewall solution protects the QALIXA Production network from the Internet. The rules on this firewall are also based on a "deny-all by default" approach: Access to systems is explicitly granted with the least amount of possible privileges. This solution prevents unauthorized access.

4 Operating System Access Control

- 4.1 Statement. Unauthorized access to operating system shall be prevented and to be restricted to only those persons who are authorized to perform systems administrations/management functions.
- 4.2 Control Instruments. The servers are hardened and accessible only to trained technical personnel. Direct access to production servers is limited to technical personnel. All technical staff members having access to production servers are identified on an authorized -personnel access list document that is updated whenever staffing changes occur. Accounts are personalized.

5 Application and Information Access Control

- 5.1 Statement. Logical access to application software and information shall be restricted to authorized users.
- 5.2 Control Instruments. Access to data and functionality within QALIXA is based on roles and permissions that determine which features of the solution a user can see and work with, and what data the user can access. The set of permissions for a user is derived from the roles mapped to that user and the groups the user may be a member of.

Internet channel security governs communications channel security between QALIXA applications, QALIXA, and other suppliers and buyers.

Communication to and from QALIXA occurs over the Internet, so customers' catalogues and transactions must be protected from interception. For increased security, QALIXA uses HTTP over Secure Socket Layer (HTTPS) for communication by default. The SSL protocol is the industry standard method for protecting communications on IP networks. QALIXA uses SSL for data encryption and server authentication. The QALIXA server is Verisign Secured.

Application security governs end-user access to the online services and information. QALIXA uses unique user IDs and passwords as the primary means of user authentication and access control. All passwords are stored encrypted in the database.

6 Handling and Processing of catalogue information

- 6.1 Statement. Preservation of Integrity and confidentiality of catalogue information provided by Seller to Buyer is essential during the handling and processing process at QALIXA. Customer submitted data and information may only be handled by authorized personal and to be safeguarded using a combination of technical access control and robust procedures.

6.2 Control Instruments. The Seller provides QALIXA with catalogue data via http(s), smtp or ftp(s) according to the formats and naming conventions set forth by QALIXA. The publishing of catalogues follows the process defined by QALIXA and the Seller. QALIXA stores all catalogue data in protected areas that can only be accessed by a limited number of people, directly involved with the processing of catalogues. Price information is only published for authorized Buyers. Sellers provide QALIXA with price information per Buyer, according to the formats and naming conventions set forth by QALIXA. The party from which the information originates is responsible for the correctness of content of the business documents.

7 Monitoring

7.1 Statement. Systems shall be monitored and information security events should be recorded to detect unauthorized information processing activities. Systems and Processes shall also be monitored in order to ensure availability.

7.2 Control Instruments. QALIXA uses a centralized monitoring product to provide maximum alerting capability. It monitors network traffic, processes system messages and alerts, application status, transaction status, etc. QALIXA uses network based intrusion detection. This technology provides logging and alert capabilities to assist in the detection of malicious acts and misuse. To monitor the actual business document flow a tool is used to give the support organization the possibility to quickly making sure that the business document flow is working correctly, and if not, where the problem is located. Limited QALIXA personnel have rights to access the monitoring systems.

8 Backup

8.1 Statement. Back-Up of data files and the ability to recover data is top priority. Accurate and complete records of back-up copies and documented restore procedures shall be in place. Frequency of back-ups should reflect the business and security requirements of information involved, and the criticality of information for continued operation. Back-ups should be given appropriate level of physical protection and media should be regularly tested to ensure they can be relied upon.

8.2 Control Instruments. QALIXA performs daily backups of the data stored. These backups do not interrupt the normal operation of QALIXA systems.

8.3 Backups are performed using disk and tape media. The media is placed in a fire proof safe.

9 Disaster recovery

9.1 Statement. In case of a severe incident the effect of the disaster must be mitigated by initiating steps to resume operation in a timely manner.

9.2 Control Instruments. QALIXA has a documented system recovery plan that outlines the approach and steps for recovering the applications. This document defines roles and responsibilities in the event of a disaster.