Qindel Security Policy

v 1.7

Qindel
16/02/2018

Table of Contents

1 Scope of the document

The aim of this document is to define the basic security policies for Qindel.

2 Change Log

Ver	*Author*	*Date*	*Change*
1.6	Nito Martínez	1/8/2017	Add policy for decommissioned equipment
1.5	Nito Martínez	15/6/2017	End user equipment policy
1.4	Nito Martínez	10/4/2017	Enhance end user security, reference external document
1.3	Nito Martínez	26/9/2011	End user security
1.1	Nito Martínez		Backup and retention periods
1.0	Nito Martínez		Initial version of the document

3 Introduction

This document tries to setup the basic security policy in Qindel. This security policy's objective is to minimize the security risk for the Qindel organization but keeping the procedures as simple as possible.

The security policy must be complemented by detailed procedures that should adhere to the policy documented here.

The security policy focuses in three main areas:

- Physical access
- Internal IT
- Internet/External IT access

Each area should develop standard procedures that depending on the technology used in each area.

4 Security committee

This committee is responsible to approve the security policy.

Any exception to this policy should be specifically approved by the security committee or by the business as such.

The security committee should be appointed by the direction.

5 Assets, risks and vulnerabilities

Here is a list of some internal assets that this policy is trying to protect:

- Financial information
- Internal documents
- Email and IM messages
- Internal software source code and binary packages
- HR internal documentation
- Hardware

The risks that this policy tries to reduce are:

- Attacks (internal and external)
- Errors
- Fraud
- Theft
- HW/SW failures

Some vulnerabilities that this policy tries to avoid are:

- Lack of user knowledge
- Clear transmissions
- Password election, and maintenance
- Technology flaws

5.1 Customer assets

This policy can be extended to include Customer specific assets:

- Financial information
- Internal documents
- Email and IM messages
- Internal software source code and binary packages
- HR internal documentation
- Hardware

Some projects might extend and enhance this policy with customer specific requirements.

6 Physical Access Security Policy

The objective is to protect physical access to the location of the following facilities:

- Qindel offices.

  The Qindel offices should have limited access to any person who is not a Qindel employee or a formal collaborator. Each visit should be logged with at least the following documentation.

  - Name of the person.
  - Entry time
  - Exit time
  - Who they are visiting
- Qindel legal and financial documentation.

  All the legal and financial documents must have a different physical access control (for example a metal key, or any other physical mechanism). The access to these documents should be limited
- Qindel servers.

  The physical access to the production servers, should be limited to the support people. These facilities should include at least:

  - Patch panel
  - Production switch
  - Internet Routers
  - Production servers
- Qindel backup information. Access to Qindel backup information, including backup tapes, backup disks or DR facilities should be the same as the support people.

7 Internal IT Logical access

Internal IT facilities are all internal applications except the following:

- Email
- Public Internet web sites (such as www.qindel.es, www.qindel.com, …)
- VOIP
- XMPP

7.1 Application access

The access to all the internal applications can be done via two ways:

- From the internal network in Qindel Office. This access can be done either via encrypted or unencrypted protocols. If unencrypted protocols are used, a switched network environment must be used.
- From the Internet or Qindel wireless network. All the external access needs to comply with the following elements:
  - It should be authenticated with user name and password
  - It needs an extra security token (X.509 certificate or other token)

  This can be done either via VPN with certificates and user and password (in the application or the VPN itself), or via web with certificate and user and password, or any similar mechanism.

7.2 User authentication, authorization and Accounting

7.2.1 User authentication

All the user authentication password hashes should be stored in the internal directory server for any internal application. Exceptions to this rule needs to be authorized by the security committee.

Access to the internal directory should be limited to a reduced number of administrators, previously approved by the security committee.

7.2.2 User authorization

Authorization to different applications by different users should be preferably handled inside the internal directory server. If the application has several levels of access these should be preferably handled by an LDAP group or role.

Exceptions to this rule should include the procedure of handling authorization mechanism and accounting mechanism.

7.2.3 User accounting

The authentication access or attempt should be documented in, at least, the directory server log. Specific accounting for each application can be documented in each application log.

7.2.4 Password policy

These are hints for the internal password policy.

- Passwords should be expired periodically
- Alphabetic passwords should be forbidden.
- The length of the password should be at least 6 characters

7.2.5 Creation, update and deletion of users

The creation of users must be approved by HR (for employees) or by director level for external employees.

External accounts must have a maximum expire date for their accounts of one year, unless otherwise specified.

User deletion must be approved by HR (for employees) or by director level for external employees.

If a user (internal or external) changes roles or projects, their new access level must be approved by HR or director level and the permissions will be changed accordingly to the new role.

7.3 Special applications

Because of their special security implications these application access should be specifically approved by the security committee:

- Email administrators.
- Documentation server administrator access.
- Accounting and billing applications access.

8 Internet Access

The internal architecture of Qindel should have at least the following elements:

- Office: This is where all the user PC and laptops are plugged in.
- VPN network: This should be considered to have the same access as the office network.
- Internet: This a non secure network
- Wireless: This should be considered an extension of Internet
- DMZ: This is where all the Internet and wireless connections go to. No data service should be located in the DMZ (relational database, LDAP server, file server, ...)
- Back end: This is where all the storage should be located such as database servers, file servers, LDAP servers, back office applications, …
- Preproduction, development networks, these can optionally exist

8.1 Policies:

- Wireless, although Qindel infrastructure should be considered Internet for the firewall policies.
- Internet connections are only possible to the DMZ, and in special cases to the test network. These connections should be encrypted when possible.
- The VPN is considered with the same privileges as the Office network
- The DMZ network should only have access to the the back end network and to the Internet. Never to the office network. In some cases access to the development network might be allowed.
- In the DMZ network there should never be database storage.
- The back end network has only access to the DMZ network.
- The office and VPN network have direct access to the Internet, DMZ and back end. The Internet network should be done via a proxy if possible.
- The preproduction network has no access to any network in the office. Only the Office network and the VPN network can have access to it.

9 Backup and Recovery

All the elements of the IT system should have a detailed backup and restore policy. The general guidelines for these are the following:

- All the user data should be backed up daily. That is in case of failure the maximum data that a user should loose should be the work of one day. As user data should be anything that a user reads or writes. Examples of such are: email, billing and accounting data, documents, reporting info, Version control system, ?
- All the system data should be backed up at least weekly. As system data should be considered the Operative Systems, the router and switches configuration, port master, and any other device in the IT infrastructure

9.1 Retention policy

The retention policy here should adhere to legal regulations needed. At least the following should be held:

- User data. The daily backup retention policy should be for at least a week.
- The weekly retention period should be at least for a month.
- And the monthly retention period should be at least for 3 months.
- Besides that there should be a 6 monthly backup and a yearly backup.

9.2 Storage policy

The backup media should be stored securely in drawer, preferably fireproof. Besides that a weekly backup should be stored outside the office.

9.3 Disaster Recovery

In case of implementation of a disaster recovery system the replication of information should be at least the time expected for the backup and recovery data.

10 End user policies and requirements

10.1 End user policies

There is a specific Qindel End User Security Policy Document that should be circulated to all Qindel employees and external collaborators that includes at least:

- Use of an antivirus is compulsory, at least in an Microsoft environment
- Keep automatic updates on the system on
- Do not open unknown email attachments
- Turn off the computer or disconnect it from the network when not in use
- Make regular backups, or store the relevant data in the corporate disk units
- Use screensavers that need to be unlocked with password. Recommended time for screen saver is 5 minutes.
- Change password regularly, do not share the password with anyone.
- Usage of clean desk policy
- Keep your keys and certificates secure.
- Access to any equipment as an Administrator or privileged user requires special security awareness
- Security is a task of everyone, if you see a security breach, please warn against it to your immediate superior.

10.2 End user equipment

The end user equipment is any equipment (desktop, laptop, mobile phone, tablet, …) that is assigned to a specific employee or external collaborator and may contain confidential data such as:

- Emails
- Internal Qindel Documents
- Internal Qindel customer information
- Internal Qindel Source Code
- Customer documents
- Customer Source Code
- Any other sensible information

Whenever the equipment is reassigned to a new employee or external collaborator, the information in the equipment must be formatted, or the data of the device must be cleared.

Optionally the information might be backed up if there are indications that there might be sensible information that needs to be maintained.

Whenever the equipment is decommissioned, the information in the equipment must be formatted, or the data of the device must be cleared.

11 Author

Nito Martínez <Nito@Qindel.ES>