INFORMATION SECURITY HANDBOOK

Version 3.1

As of May 2019

Approved by	Name	Date
CIO	Justin Miller	05/19
ISO	Justin Miller	05/19
Managers	Vivek Kohli, Surendra Singh	05/19

Information Security Policy

A fundamental aspect of Security within Quark Software Inc is to protect information that is sensitive or crucial for its operations. As such Quark Software Inc has defined this Information Security Policy to describe the intentions and expectations of management to protect such information. This Information Security Policy concerns all employees at Quark Software Inc.

The operations and business of Quark Software Inc is to a large extent dependent on a well-functioning IT environment. A substantial amount of information is created and managed on a daily basis within the Quark Software Inc environment that has to be made available in a reliable manner to conduct its business. It is imperative that Quark Software Inc comply to its Information Security Policy as a governing principle to assure the markets it serves that all information used in conducting its business and operations. Quark Software Inc seeks to adhere to its Information Security Policy:

- By striving to have the information it needs through an IT environment that is always available – interruptions in the business processes and the availability of the IT systems will mean lost time, idle resources, poor quality and delivery of products and services. Moreover, the interruptions may damage the Quark Software Inc brand.
- By ensuring that the management of business and customer information is reliable and of high quality – errors in the handling of information may lead to increased costs and lost confidence in the ability of Quark Software Inc to serve its markets well.
- By making sure that confidential information can only be accessible by authorized employees and customers – confidential information in the wrong hands can be used to the detriment of Quark Software Inc and its customers.
- By using efficient routines to prevent, detect and manage possible security incidents or other emergent situations that may occur - the use of these routines will reduce the consequences and costs of an incident.
- By managing information and the IT environment according to laws and requirements of the authorities in respective countries together with other branch requirements.
- By seeking to gain assurance from our business partners that their work and IT environment will secure any information concerning Quark Software Inc within the framework of Quark Software Inc's Information Security Policy.

All security solutions and associated routines shall be expedient and cost efficient and governed under the same policies and guidelines as all other investments or improvements. The need for security shall therefore be assessed based on the consequences that may occur if a protective measure such as a security solution or routine is missing. This assessment shall be based on four main goals regarding our information security:

- Availability – the necessity of having the information available.
- Integrity – the necessity of the information being current, correct and complete.
- Confidentiality - the necessity of having the information only available for authorized users.
- Accountability – the necessity of being able to establish who has had access to specific information, when this occurred and what the information was used for.

The Information Security Policy shall be the foundation for more detailed security rules regarding information and the IT environment.

Each employee is responsible for compliance with the Information Security Policy and the rules in the

Information Security Handbook. Training and distribution of information will contribute to a good understanding and awareness of the information security rules.

Our business is constantly changing, due to new market demands and conditions together with a rapid development of new technology. These changes can result in new risks facing our business and consequently changing needs and requirements of information security. Thus, in connection with changes, analysis needs to be made to establish whether adjustments have to be made in the management of security.

Information security is mainly based on common sense, good judgment and effective routines, where each employee’s contribution is crucial. Taken together, these are important prerequisites that contribute to ensuring confidence in our business and significantly improve the possibility to meet our business objectives.

Change history

Date	Version	Created / Modified by	Description of change
2017-08-11	1.0	Jim Haggarty	Initial policy document created
2018-05-02	2.0	Jim Haggarty	Annual review and update; added sections for social media usage.
2018-08-08	2.0	Vivek Kohli	Added Form for Acceptance / tracking
2019-05-06	3.0	Vivek Kohli	Annual Review and Update
2019-05-21	3.1	Vivek Kohli	Added Avoiding Social Engineering and Phishing attacks and Information tips in different sections of the handbook.

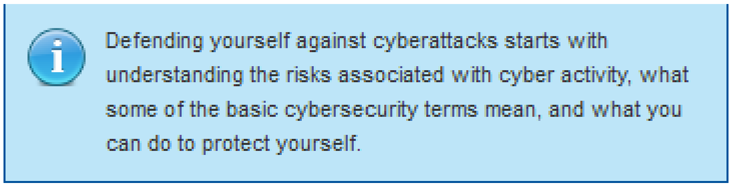
Table of Contents

1. Introduction to Information Security

1.1 General

This chapter gives a general description of information security, the objectives and approach to information security at Quark Software Inc and the extent of the work. The handbook defines the basic rules for information security within Quark Software Inc, the lowest expected level. The chapter also includes reading instructions for the information security handbook. This Information Security handbook concerns all employees at Quark Software Inc. It also concerns all our suppliers of IT services and operations as well as external resources using Quark Software Inc's information and IT systems.

In this handbook the terms protection, protective measure and control are used, meaning all actions, workarounds, routines and solutions made to avoid having information spread to unauthorized people, to avoid errors in the information and to make sure the information is available.



Defending yourself against cyberattacks starts with understanding the risks associated with cyber activity, what some of the basic cybersecurity terms mean, and what you can do to protect yourself.

1.2 What is Information Security?

Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Information can exist in many forms and formats. There are many possible threats to the information, for example documents can be stolen, intrusion via the Internet, viruses transmitted by e-mail and negligence within the organization. The risks and threats to our information are constantly changing because of the ongoing changes in the surrounding world, rapid new technical developments and arising new business opportunities. In general, technical developments give many new opportunities, but at the same time many new risks and threats may appear.

In order to control the risks and threats to our information we must protect the information; we introduce *Information Security*. The information is often managed, stored and transmitted using IT systems and networks, therefore information security also includes *IT security*. The protection consists of technical solutions (e.g. firewalls, antivirus, passwords) as well as administrative procedures (e.g. authorization, access controls and reporting routines, information management). The picture below illustrates examples of threats and risks to the information and possible methods to protect the information.

CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
HUMAN ERROR
TROJAN
HACKING
CYBERCRIMINALS
TROJAN
SYSTEM PENETRATION
YOUR DATA SAFETY
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
SPYWARE
SOFTWARE ERROR
STOLEN INFORMATION
CYBER ATTACKS
PASSWORD CRACKING
FRAUD
ADWARE
CYBERSTALKING

1.3 Objectives of the Information Security at Quark Software Inc

The Information Security Policy defines four main objectives for the information security: Confidentiality, Integrity, Availability and Accountability. All protective measures used to protect the information at Quark Software Inc are used to secure that these objectives are reached. In order to establish what type of control that is necessary, it is essential to identify and understand all the threats and risks that may occur. E.g. how can someone access the information without being authorized, change the information incorrectly or make the information inaccessible?

The table below describes the objectives with information security and some threats and risks:

	Objectives of the Information Security:	**Threats to the objectives (examples):**
Confidentiality	*The information shall only be available for authorized employees and customers*	*Theft of paper documents*, *Wire-tapping or bugging.* *Unauthorized access to IT-systems*
Integrity	*The information shall be reliable, correct and complete*	*Unauthorized tampering of information* *Unintentional modification of information* *Computer virus*
Availability	*The information must be available according to the needs of the business*	*Power cuts* *Systems errors* *Unintentional modification of information* *Problems with the network or the Internet access*
Accountability	*It must be possible to establish afterwards who has accessed the information, what was done with it and when it occurred.*	*Accidental update or deletion of logged information*

The protective measures selected must be in proportion to the risks that the business is exposed to. That is, it shall not be more expensive to install and use the protective measure than the cost that would arise if the risk(s) occurred.

The Quark Software Inc information security handbook outlines the information security ambition at Quark Software Inc. The compliance with the handbook will happen gradually along with that the prerequisites for compliance is being established.

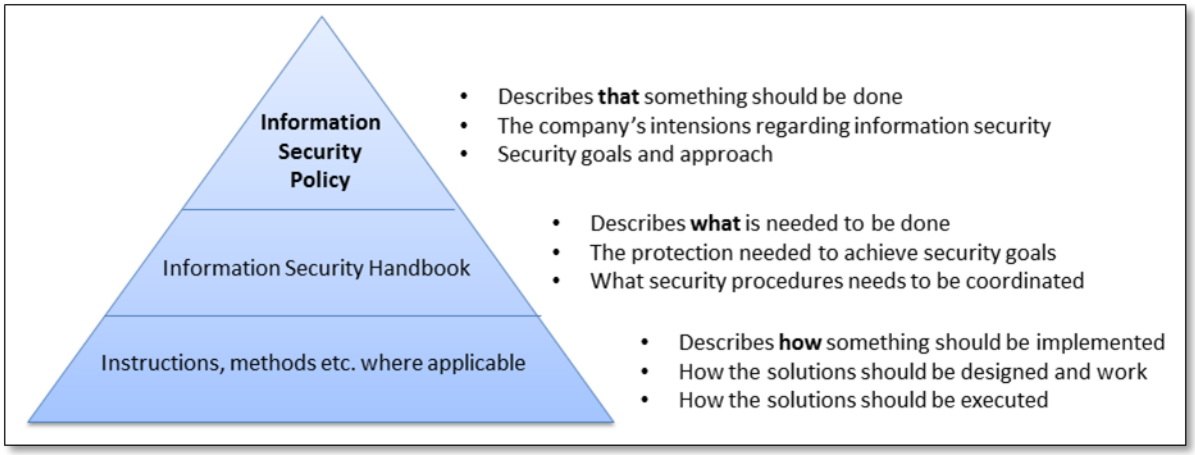
1.4 Content of the Information Security work

To be able to reach the objectives of the information security, different types of protective measures and controls must be implemented. They must be implemented for digital information in the IT environment, for paper documents, and where possible, for oral information. In general, information security includes the following:

- Access to information – ensure that only authorized personnel can access and update the information.
- Continuous management of information - to ensure that critical information is protected when used in the daily business.
- Processing, storing and distribution of information in the IT environment – to ensure that IT systems and networks are available, and that the information is managed correctly.
- Physically secure the information – to ensure that only authorized personnel get Physical access to the information.
- Management of incidents and plans for crises – to ensure that security incidents are discovered and handled. In case of serious incidents, like a fire, the business must be able to operate at least to a limited extent.
- Risk analysis and evaluation – to verify that all relevant risks are controlled by protective measures.

1.5 The Information Security Framework

The structure of the Information security documentation at Quark Software Inc is illustrated in the following picture:



Information Security Policy

- Describes **that** something should be done
- The company's intensions regarding information security
- Security goals and approach

Information Security Handbook

- Describes **what** is needed to be done
- The protection needed to achieve security goals
- What security procedures needs to be coordinated

Instructions, methods etc. where applicable

- Describes **how** something should be implemented
- How the solutions should be designed and work
- How the solutions should be executed

The Information Security Handbook describes rules regarding routines and security measures that must be implemented to achieve the objectives established in the Information Security Policy. The intention of the handbook is not to describe in detail how the procedures and measures shall be designed, but to describe the minimum expected level of information security. Procedures and solutions must be adjusted to the daily business and activities in the organization. The CIO (Information Security Manager), ISO is responsible for the handbook.

With guidance from the information security handbook instructions, methods and local rules shall be developed, which in detail describes how security procedures and measures shall be designed and applied in order to fulfill the rules in the handbook. The detailed instructions, methods and local rules shall be produced by the function or role responsible for the function or component that needs to be protected

1.6 Reading instructions to the Information security handbook

Chapter		Receiver	Brief description
	Information Security Policy	All employees	Clarifies the Chief Executive Officer's view on information security.
1	**Introduction to Information Security**	All employees	Brief description of information security.
2	**Information Security Responsibilities**	All employees	Roles and responsibilities for information security.
3	**Employee's guide to Information Security**	All employees	Rules for employees.
4	**Investigation of Information Security risks**	Information owners, Function owners, IT managers	Identification of risks to implement adequate protection.
5	**Information access control**	Information owners, Function owners, Technical owners, IT managers	Rules to establish who has access to specific information.
6	**System, communications and network security**	Function owner, Technical owners, IT personnel with systems, network and operational responsibilities	Rules concerning operation, maintenance and support of IT systems, applications, network and related equipment.
7	**System development and procurement of standard systems**	Information owners, Function owners, Technical owners, IT managers, Project managers and members	Rules concerning development of software in- house, at external parties or procurement of standard systems.

8	**Physical security for information and systems**	Function owner, Technical owners, personnel responsible for the Physical security.	Rules regarding the Physical protection of information and IT systems.
9	**Information Security in the personnel administration process**	Staff with personnel responsibilities	Rules regarding the personnel administration process
10	**Incident handling and reporting**	All users of IT systems	Rules regarding how to report and manage incidents concerning the information security.
11	**Email & Social Media usage**	All users of IT systems	Rules regarding the use of email and social media
12	**Encryption**	All users of IT systems	Rules regarding the use of encryption in different situations
13	**Data privacy**	Information owners, Function owners, IT managers and IT personnel, and managers	Rules regarding Quark Software Inc principles for data privacy
14	**Compliance and follow-up of Information Security**	IT managers, Managers	Rules regarding compliance to and follow-up of Information Security Policies
15	**Appendix A. (List of Policies)**	All users of IT systems	Additional detailed policies (cloud services)
16	**Acknowledge and Acceptance**	All Employees	Acknowledge reading through and understanding the policy followed by submission.

2. Information Security Responsibilities

2.1 General

The purpose of this chapter is to describe the information security responsibility at Quark Software Inc and its coordination. The purpose of the overall security work at Quark Software Inc is to protect:

- The lives and health of employees and customers.
- The company's business in the short run and in the long run.
- The company's property.
- The company's name, reputation and trademarks.
- Assets and resources in the company, which handle and use the information.
- The company's business processes and information flows.
- Customer information.

2.2 Overall Responsibilities

The Chief Information Officer (CIO) of the company has the ultimate responsibility for information security at Quark Software Inc, and it is the management's responsibility to ensure a well-functioning organization for the information security work. Management shall initiate and support the security work with resources, so that the business needs for protection and security are fulfilled*.* The CIO shall establish the directions and objectives of the information security in the Information Security Policy.

Information security is a part of the overall security work at Quark Software Inc. Information security includes protecting the assets and resources that manage, store or in some other way use the information of our business. The business organization has the operational responsibility for the information security, meaning that it is the business and the business responsible individuals that are responsible for the implementation and the conformity to the rules.

2.3 Information Security Responsibility

In each Quark Software legal entity, the CIO is responsible for ensuring that the company fulfills the rules and requirements established in the policy and the handbook. To summarize, the responsibility includes the following*:*

- Allocate resources to ensure that the rules for information security in the handbook get communicated, applied and maintained.
- Allocate and plan resources so that planned activities in the annual plan for information security are implemented.
- Ensure that sufficient information security responsibility is established and communicated, like appointing information and functional owners to the information and business critical systems.

The ISO of the Company has the overall responsibility for and coordination of the Information

Security at Quark Software Inc. To summarize, the responsibility includes the following:

- Ensure that the basic level of security is covered for the IT systems and networks at Quark Software Inc. The ISO shall supply the necessary conditions in order to implement the IT related requirements and rules defined in the policy and handbook together with requirements set up by the functional owners.
- Make decisions regarding serious IT security incidents.
- Ensure that our suppliers of IT services and operations fulfill Quark Software Inc's requirements regarding availability, confidentiality, integrity and accountability for the central systems.
- Being responsible for the company's Information security handbook, which includes ensuring that the rules for information security continuously are developed, communicated, and updated.
- Maintaining an annual plan for information security, with directions from the rules in the information handbook, to be approved by management.
- Being the method owner for important information security methods, like risk analysis.
- Report serious information security incidents to the company management.
- If necessary give exemptions from policies, guidelines or instructions.
- Initiate the development of remediation plans based on results from any review or audit, internal as well as external.
- Being the contact for the information security responsible persons in the company.
- Assess the secure installation and maintenance of encryption controls at the company.
- Assess key management processes.
- Reviews and approves appropriate encryption exception requests.

The IT managers in the company are responsible for ensuring that the IT environment in the company fulfills the rules and requirements in the policy and the handbook. To summarize, the responsibility includes the following:

- Ensure that the local system and network resource of the company fulfills the IT security rules described in this handbook.
- Organize and assign IT security responsibilities according to this handbook.
- Ensure that the function owner's requirements regarding availability, confidentiality, integrity and accountability are reached from an operational standpoint.
- Initiate reviews of the IT security level at the company and ensure that identified weaknesses are removed.

Information owner, for each set of information there shall be an information owner who is responsible for the information security. The responsibility includes ensuring that risk analysis is performed for the information he/she is responsible for and for classification of the information. The information owner also approves access/access levels to the information he/she is responsible for. The responsibility is a part of the normal responsibility that the manager for a business area has, when the business acquires, creates, processes and/or maintains information. As long as the information remains within the business area the information owner is responsible for it.

Function owner, for each IT system a function owner shall be appointed, who is responsible for information security on the aspect of confidentiality, integrity, availability and accountability regarding his/her IT system. The function owner is responsible for performing risk analysis for the system and its information, and that the information owner's requirements are taken into consideration. The responsibility also includes coming to an agreement regarding additional security measures with the IT manager of the company and the technical owner.

Technical owner, for each IT system a technical owner shall be appointed, who is responsible for an optimal function in the area of system development and maintenance as well as systems operations. The responsibility includes maintaining the basic level of security as described in this handbook and to come to an agreement with the function owner regarding the implementation of additional security measures. It also includes the following responsibilities:

- Timely realization of new functionality and changes as defined by the function owner.
- Arranging, together with the function owner, the required operational facilities.
- Monitors technical problems for immediate repair.
- Implementing any additional IT related information security requirements that have been agreed with the function owner.

Each manager with personnel responsibilities is responsible for ensuring that:

- The employee is informed of and follows the employee rules regarding information security.
- Contractors and other external staff follow the rules in his handbook.
- The employee has the opportunity to participate in security training.
- Time is allocated for issues regarding information security at the department meetings.

Each employee has a responsibility to follow the rules for information security outlined in this handbook. The employee shall in her work always consider what is best for Quark Software Inc. The employee's responsibilities are summarized in *chapter 3 Employee's guide to Information Security.* In short, the responsibility includes the following:

- Protect confidential and strictly confidential information from being accessed by unauthorized people.
- Use e-mail and the Internet primarily for work related purposes.
- Protect passwords, keys and other equipment used to access the IT environment, buildings or other facilities.
- Report security incidents.

2.4 Guidance to the rules for each responsibility

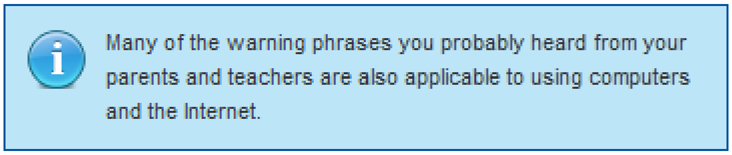
The following table gives an overview of the main chapters concerning the information security responsibility and rules connected to a specific role in the organization.

Role	Responsibilities and the associated rules are described in
Information owner	4 - Investigation of Information Security risks 5 - Information access control 7 - System development and procurement of standard systems
Function owner	4 - Investigation of Information Security risks 5 - Information access control 6 - System, communications and network security 7 - System development and procurement of standard systems 8 - Physical security for information and systems
Technical owner	5 - Information access control 6 - System, communications and network security 7 - System development and procurement of standard systems 8 - Physical security for information and systems
Manager	5 - Information access control 9 - Information Security in the personnel administration process
Employee (all)	3 - Employee's guide to Information Security 10 - Incident handling and reporting 11 - Email 12 - Encryption
Project managers	4 - Investigation of Information Security risks 7 - System development and procurement of standard systems
Personnel with Physical security responsibilities	8 - Physical security for information and systems
Internal audit	14 - Compliance and follow-up of Information Security

3. Employee’s guide to Information Security

3.1 General

The purpose of this chapter is to describe what you, as an employee and a user of the IT environment and the information at Quark Software Inc must be aware of and take into consideration in your daily work.



Many of the warning phrases you probably heard from your parents and teachers are also applicable to using computers and the Internet.

3.2 Employee’s responsibilities

The table below shows a comprehensive description of what you need to take into consideration in order to protect the information and the IT environment.

Protect sensitive information	You must handle sensitive information with precaution to avoid having the information fall into wrong hands. This necessitates protective measures when e.g. printing, archiving or distributing information.
Handle your password and user account in a secure manner	A secret and unique personal password is one of the best protections to avoid unauthorized access to your computer and the IT environment.
Use the Internet and e-mail with common sense	The risk of malware is overwhelming when using the Internet and e-mail. Some web pages are associated with additional risks. Therefore, all use of Internet and e-mail shall be performed with precaution.
Protect your computer equipment and other accessories	Thefts of PCs and mobile phones are very costly. Moreover, if the equipment contains sensitive information, there is a risk it will fall into wrong hands. For this reason, you shall never leave this kind of equipment unguarded at public places, in the car etc. When storing confidential data on your PC, the information must be protected with encryption.
Report security incidents and suspicions of incidents	In case of a security incident, like a virus attack, we must attend to the problem immediately and find a solution. Therefore, it is very important that you contact internal IT as quickly as possible when you find or suspect a security problem.

The following section describes how you shall proceed to fulfill your responsibilities.

3.3 How to protect confidential information

If confidential information falls into wrong hands it may lead to serious consequences for Quark Software Inc's business. Thus, we distinguish confidential information from other less crucial information in order to give better protection to the confidential.

At Quark Software Inc we use the following information classes:

Information class	Description	Examples
Open Information	The information is public and can be distributed to outsiders without causing any damage or other negative consequences for Quark Software Inc.	• Advertising handouts • Published information • Description of goods
Intra Company Information	Only employees of Quark Software Inc shall share the information. Spreading of the information outside Quark Software Inc does not cause any damage but shall be avoided	• Internal messages • The Information security handbook • Internal address book
Confidential information	The information shall not be spread outside the group of colleagues that need the information in their work. Spreading of the information to outsiders can cause negative consequences such as bad-will, lost revenue, increased costs etc.	• Information about customer or supplier • Project information • System documentation with crucial data.
Strictly confidential information	The information must only be accessed and handled by a few directly involved and authorized coworkers at Quark Software Inc. Spreading of the information to outsiders may cause serious consequences like negative publicity in the media, substantial costs, claims, lost market shares etc.	• Business plans • Business strategy • Passwords • Payroll

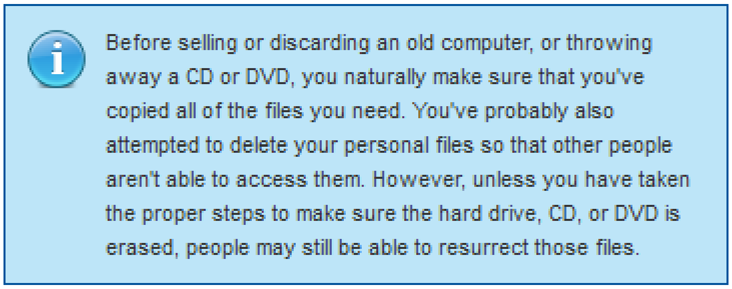
In general, the following rules apply for all information:

- Strictly confidential and confidential information must be labeled with the information class.
- Information not labeled with a class shall be handled as intra-company information.
- Intra-company and open information shall be handled with good judgment and common sense.

The following page describes how you shall handle information classified as strictly confidential or confidential.

3.3.1 When you need to protect the information

The table below gives an overview of how strictly confidential and confidential information shall be managed in different situations. If you are insecure on how to manage the information, contact your manager.



Before selling or discarding an old computer, or throwing away a CD or DVD, you naturally make sure that you've copied all of the files you need. You've probably also attempted to delete your personal files so that other people aren't able to access them. However, unless you have taken the proper steps to make sure the hard drive, CD, or DVD is erased, people may still be able to resurrect those files.

When you are going to:	Confidential information	Strictly confidential information
Archive or store	• Paper documents, diskettes, or CD-ROM shall be in a locked storage area or locked cupboard. • Data files shall be stored on a separate file server dedicated for information storage. • Information on PCs shall be stored encrypted.	• Paper documents, diskettes and CD-ROMs must be locked in theft safe cupboard, only accessible by authorized coworkers. • Data files shall be stored in an encrypted format on workstations, fileservers and portable PCs.
Read	• The information owner responsible for the information decides who has the right to read the information.	• The information owner responsible for the information approves who has the right to read the information. • Contact internal IT to limit the reading access to a data file. • On paper documents the authorized receiver of the document must be specified.
Update	• On paper documents it must be specified who has updated the document and when it was done. • In data files it must be specified who has updated the file and when it was done.	• Only the person issuing or owning the paper document or data file has the right to update the information, unless someone else has been authorized to do it. Contact internal IT for update protection of data files.

Destroy or delete	• Paper documents must be destroyed in a paper-shredder or collected in the office’s paper collection if it is sealed and the documents later securely destroyed. • Contact internal IT for secure deletion of data files, diskettes, CDs etc.	• Paper documents shall be destroyed in a paper shredder. • Contact internal IT for secure deletion of data files, diskettes, CDs etc.
Distribute or send	• External mail: In a well-sealed envelope. • Internal mail outside the department: In a well-sealed envelope. • Fax: Agree with the receiver to stand by the fax machine when the information is sent. Request a receipt. • E-mail: Must be in an encrypted format when sent to external e-mail addresses (outside Quark Software Inc).	• External mail: In a well-sealed envelope sent as a registered letter. • Internal mail: Personal delivery, otherwise in a well-sealed envelope • Fax: To be avoided unless the receiver has a personal fax machine. • E-mail: Digitally sign and send the e-mail encrypted. The e-mail shall also be stored in an encrypted format in the mailbox.
Print	• Employee must “guard” the printer to make sure no one else can access the document	• Personal printer in the receiver’s private office.

3.3.2 Keep in mind that other people can hear and see

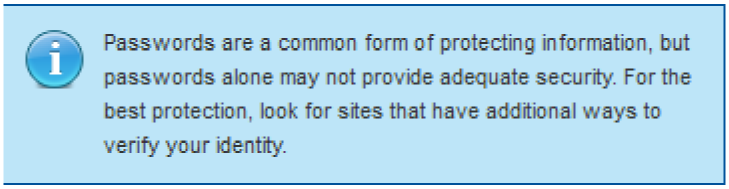
Never discuss confidential information in public places or where there is a risk that someone can overhear what is said. The same precaution is necessary when communicating using telephones, mobile phones, answering machines or SMS. Moreover, do not read confidential documents (paper documents or on the PC screen) at public places, subways, airports, restaurants or other places where there is a risk that someone will be able to see the information.

3.3.3 When you have a visitor

Visitors shall be welcomed at the entrance and escorted during the whole visit at the office. All visitors must be signed in. Keep in mind that the visitor shall not have the possibility to view any sensitive information. Do not hesitate to ask visitors or people you do not recognize who they are visiting and try to guide them.

3.4 How to protect your password and user account

The most common way for an intruder to access confidential information in IT systems is by obtaining someone’s password, one way or the other. Therefore, it is essential to keep your password secret and that you do not choose simple passwords, which someone can easily figure out.

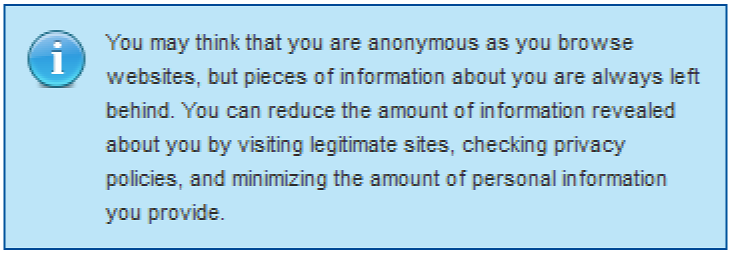


Passwords are a common form of protecting information, but passwords alone may not provide adequate security. For the best protection, look for sites that have additional ways to verify your identity.

The password is personal and must be kept secret	• Never reveal your password to anyone. If you suspect that someone knows your password, you must change it at once. • Never write down your password or keep it in such a way that someone else can access it.
The user account is personal	Do not share your user account with other users. If you do, all activities other users perform will be registered in your name and likewise be your responsibility.
The password must be difficult to guess	It is quite easy for a potential intruder to quickly reveal a short and simple password. When selecting a password, you shall for example not choose: • The name of family members, initials or your car's registration number. • User-id, User name, company-ID or another system identifier. • Numbers or letters in a straight row, e.g. 123456 or ABCDEF.
Only use the password at Quark Software Inc	The password used at Quark Software Inc shall not be used anywhere else, like for your private e-mail or some service on the Internet. Unauthorized users, e.g. hackers, can use the password, depending on how reliable the service is. Enable Multi Factor Authentication (MFA or 2FA) if supported.
Make sure the screen saver is activated	When you leave your computer unattended you must activate the screen saver manually. The screen saver shall be automatically activated within 10 minutes of inactivity.

3.5 How to use the Internet and e-mail with common sense

The use of the Internet and e-mail has become a frequent part of our daily work. However, at the same time these activities generate risks to our business. The Internet is a public network with millions of users. We must utilize all the possibilities and advantages with the Internet but avoid unnecessary risks. Each of us has a responsibility to limit the risks related to the use of the Internet and e-mail.



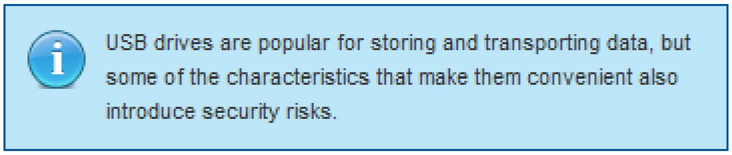
You may think that you are anonymous as you browse websites, but pieces of information about you are always left behind. You can reduce the amount of information revealed about you by visiting legitimate sites, checking privacy policies, and minimizing the amount of personal information you provide.

Visit Internet sites with good judgment	• The use of the Internet shall primarily be work related. • Be aware of that you are leaving tracks when visiting different sites on the Internet. Other users on the Internet can track your visit. Thus, do never visit sites with unsuitable or provocative content. • Quark Software Inc reserves the right to monitor the Internet traffic at the company.
Be careful when using instant messaging	• Be aware that IM can be used to spread viruses or other malware. Use precaution when opening files or clicking on links. You must only use company approved IM services. • The use of external IM services is prohibited.
Use precaution when downloading files	• Use precaution when down loading files, both concerning the content and the size. Files not related to work, e.g. music and games, are not allowed to download. These types of files can seriously affect the performance and availability of the network.
Be aware of what you are sending	• Confidential and strictly confidential information must be protected when sending an e-mail and attaching this kind of information (see section 3.3, How to protect confidential information).
Do not auto forward your e-mail	• To use auto forward to an external mailbox, such as hotmail, is not allowed. • Be cautious with registering your e-mail address at Quark Software Inc on external databases on the Internet, since these are often used for spamming i.e. the spreading of junk mail. Consider unsubscribing from marketing emails that are no longer of interest.
Be cautious with your e- mail	• Do not open attachments and/or links if you don’t recognize the senders e-mail address or identity. • Handle e-mail and attachments with strange names or content with skepticism. Be aware of that the sender’s e-mail address can easily be falsified. • Do never forward questionable mail or chain letters to colleagues at Quark Software Inc or to external users.

3.6 How to protect the computer equipment and other accessories

You are responsible for handling and keeping your computer equipment in a responsible manner to minimize the risks for malfunction and theft. Computer equipment includes the following:

- Portable computers (Laptops).
- Desktop computers (stationary PC's).
- Mobile phones.
- Removable media


USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks.

In order to protect your computer equipment, you shall keep the following in mind:

Never leave your computer turned on when leaving the office after work	• Turn off (or lock) the computer when leaving the office.
Never leave your computer unguarded during business trips etc.	• To the extent it is practically possible, you shall never leave your portable PC unattended.
Make sure the virus scan is activated and that it is updated regularly	• Make sure the virus scan is activated and that it is updated regularly. The computer normally handles this automatically.
Disks on laptops must be encrypted.	• If you're carrying a laptop outside the office, the disk must be encrypted. A full-disk encryption solution must be installed.
Removable devices (CD:s, DVD:s, flash drives, USB tokens, portables discs) containing confidential information must be encrypted.	• If you're storing confidential information on a removable device, the device must be encrypted.
Never install software unless they are approved by the IT department	• It is prohibited to install unapproved software on equipment belonging to Quark Software Inc unless internal IT approves it.
Backup information regularly if you cannot store it on the network	• If you must store information locally, e.g. on a Laptop, make sure to make a backup regularly. If the information is stored on the network this is handled automatically. If you're using a local external hard drive for backup, the device must be encrypted. The encryption key must be centrally stored within the IT department.

3.7 How to report security incidents

If you find or suspect some kind of weakness or incident, you must contact your closest manager and internal IT immediately.

When you suspect that you have received an e-mail or attachment infected by a virus or phishing links, or if you notice some kind of abnormal behavior from your computer when using the Internet or e-mail, you must immediately do the following:

- Document how the computer behaves abnormally and take screenshots of any messages you get on the screen.
- Stop using the computer, disconnect from the network and inform internal IT and wait for further instructions.

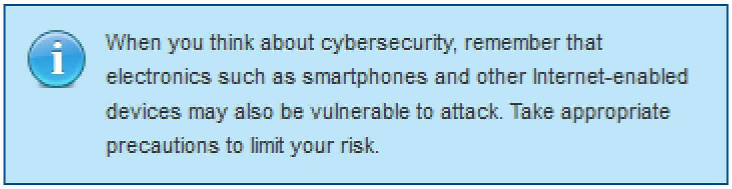
Never test if your suspicion is correct – never use a file you suspect contains viruses. If your suspicion is correct the virus can cause substantial damage to Quark Software Inc.

3.8 Finally

At Quark Software Inc we help each other. If you find forgotten paper documents or discover some other possible security problem, make sure it is taken care of. Contact the information security manager or your manager if you are not sure how to solve the problem.

Quark Software Inc owns the computer equipment and all the stored information. Quark Software Inc has the right to access and review the content of mailboxes and folders. However, such a procedure will only be performed if there is a suspicion of a crime or if there is a security related problem, such as viruses. All reviews must be approved in advance by the information security manager. Moreover, all Internet access and sites that are visited are logged.

If you have any opinions or if you want to discuss the rules in this handbook, please contact the ISO.



When you think about cybersecurity, remember that electronics such as smartphones and other Internet-enabled devices may also be vulnerable to attack. Take appropriate precautions to limit your risk.

4. Investigation of Information Security risks

4.1 General

The objective of the information security work at Quark Software Inc is to protect sensitive and crucial information from various threats, which can lead to that information to spread, updated or deleted in an unintentional way. An essential part of this work is to identify the threats and risks, which the information is exposed to. This chapter describes the fundamental requirements for:

- Risk analysis.
- Information classification.

This handbook describes the *basic level of security* at Quark Software Inc, that is the protective measures that shall be implemented for all the information (see also chapter 1 Introduction to Information Security). In addition to the basic level of security, each person responsible for an area has to evaluate if this security level is sufficient for the information processed in his/her area of responsibility. This is usually done in a ***risk analysis***.

In addition, all individuals (information owners) have to analyze the information processed within their area of responsibility. This will determine the sensitive/crucial information that must be managed in a secure way. This is usually done via an ***information classification***.

4.2 Responsibility

The ISO at Quark Software Inc is responsible for supplying the method to be used in the risk analysis within the organization, and to define the overall structure for information classification and the belonging rules. The responsibility also includes giving continuous support and advice to the organization within these areas.

The information owner has to ensure that risk analysis is performed for the information he/she is responsible for and for classification of the information.

The function owner is responsible that risk analysis is performed for the system and its information, and that the information owner's requirements are taken into consideration. The responsibility also includes assuring that the basic security level is maintained and to come to an agreement regarding the IT security with the IT manager of the company and the technical owner.

The *technical owner* is responsible for maintaining the basic security level as described in this handbook, and for implementing any additional IT related security requirements that have been agreed with the function owner.

4.3 Risk analysis

4.3.1 General

Some risks and threats are unique to different systems and processes. For example, an Internet application is exposed to different risks and threats than an internal accounting system. In many cases the basic level of security is sufficient, however many systems and business processes may need *extended security*, due to specific risk exposure or information requiring confidentiality, integrity and/or availability. The basic level of security may need to be complemented and strengthened; therefore a specific risk analysis needs to be performed for the system and its information.

Risks are often described in terms of threat, probability and consequence. Possible threats to the information can be for example:

- Unauthorized access to our IT systems.
- The IT systems are infected by computer viruses.
- The equipment in the server room is damaged by water leakage, damp or dust.
- An employee forgets a confidential report in the departure hall at the airport.

Some incidents are more serious than others – *the consequences* of these incidents are greater when the damage to Quark Software Inc is more severe. The spreading of confidential information regarding business plans to unauthorized people causes much more damage to Quark Software Inc, compared to if internal information is spread to the public. Threats also have different probabilities to occur.

The greater the consequence of a threat that is realized is, and the higher the probability of the threat to occur is, the higher is the risk for the business. Thus, risks are a combined assessment of probability and consequence.

4.3.2 Risk analysis at Quark Software Inc

Risk analysis shall be performed periodically for all systems and associated information at Quark Software Inc. As a general rule, risk analysis shall be performed when there are:

- Larger changes in the organization.
- Implementation or development of new services in the organization.
- Significant changes in the IT systems or the applications.
- New development or acquiring of IT systems or applications.

The methods used for risk analysis at Quark Software Inc shall:

- Be approved by the ISO.
- Be documented and easy to understand.
- Identify risks and threats.
- Involve relevant key persons (e.g. information owner, functional owner, technical owner, users and IT staff).

- Result in information security requirements that shall be implemented for the IT system and its information. The requirements for confidentiality, integrity, availability and accountability must be established.

The information security requirements for the system and its information shall at least fulfill the basic level of security specified in this handbook. The information security requirements shall be documented. If the requirements demand major changes to the IT environment as a whole, the ISO of the company shall also be involved.

The risk analysis shall at least result in the following:

- Documentation of risks concerning the IT systems and its information.
- The risks shall be prioritized based on the combined assessment of their probability and consequence.
- Establish if the basic level of security specified in this handbook is enough to manage the risks.
- Identify the risk areas where the basic level of security is not enough.
- Report of the results to senior management.
- A remediation plan to address issues and risk areas where controls are deemed not enough.

4.4 Information classification

4.4.1 General

The purpose of the information classification is to identify the information that is so sensitive or crucial that it requires protective measures when handled. For example, sending confidential reports using registered letters, put business plans in the shredder instead of the wastepaper basket etc.

Information classification and risk analysis are closely connected. During the risk analysis, information that is crucial to the analyzed function, system or process is often discussed. Therefore, the result of the risk analysis is of great support during the information classification. Likewise, the result from the information classification can be of great support during the risk analysis, since the information classification has identified the information that requires further analysis.

4.4.2 Information classes

Information and systems shall be classified based on three classes:

- Confidentiality
- Availability
- Integrity.

The following requirements of basic level of security must be acquired:

- All information, on paper as well as digital, must be classified based on confidentiality and availability (see information classes on the following page).
- Integrity class shall be established for the systems and their information

The information owner establishes the correct class concerning *Confidentiality.* This can be an employee when creating the information, for example a word document, or appointed information owners in the organization who are responsible for the information that is created and managed using the IT systems.

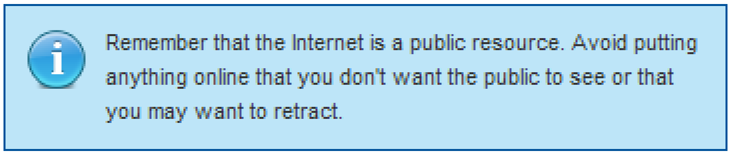
The functional owner in consultation with the information owner, the technical owner and the system developers usually do the classification of the requirements for *Availability* and *Integrity.* Classification is usually done for the software and hardware that process, store and transfer the information.

The information classification shall at least result in the following:

- Established Confidentiality class for the information that will be managed in the system and by the associated manual routines.
- Rules for employees when handling information classified as Strictly Confidential or Confidential. (The basic level of security for this type of information is described in the employee's guide 3.3 How to protect confidential information).
- Established Availability class for the components (hard- and software), which support the system and carry out its functionality.
- Safety rules for the components classified as Very Critical or Critical.

4.4.2.1 Confidentiality

At Quark Software Inc four *Confidentiality classes* are used for the information:



Remember that the Internet is a public resource. Avoid putting anything online that you don't want the public to see or that you may want to retract.

Integrity	Meaning	Examples
Strictly confidential information (S1) *Shall be labeled " Strictly Confidential"*	The information must only be accessed and handled by a few directly involved and authorized coworkers at Quark Software Inc. Spreading of the information to outsiders may cause *very serious consequences*, such as bad-will, lost customers, lost revenue and decreased stock value etc.	• Business plan • Strategies • Password • Encryption keys
Confidential information (S2) *Shall be labeled " Confidential"*	The information must not be spread outside the group of colleagues that need the information in their work. Spreading of the information to outsiders can cause *serious consequences,* such as bad-will, lost customers, lost revenue and decreased stock value etc.	• Customer related information • Distributor related information

Intra-company information (S3)	The employees of Quark Software Inc shall only share the information. Spreading of the information outside Quark Software Inc will only cause *minor consequences* but shall be avoided.	• Internal messages • Internal address book
Open information (S4)	The information is public. Spreading of the information will not have any consequences for Quark Software Inc.	• Advertising handout • Published information
Associated protective measures and rules shall be developed for the information classified as Strictly Confidential or Confidential. The rules for basic security for these classes are described in the employee’s guide 3.3 How to protect confidential information.		

4.4.2.2 Availability

The following *Availability classes* are used for the information at Quark Software Inc:

Availability	Meaning	Examples
Very Critical (T1)	The information, software and equipment must be available within 4 hours after the business area responsible for the information has made a decision.	• Network equipment • Backup copies • Application software • Operational system • System documentation • Job schedule
Critical (T2)	The information, software and equipment must be available within 24 hours after the business area responsible for the information has made a decision.	
Less Critical (T3)	The information, software and equipment must be available within 1–3 days after the business area responsible the information has made a decision.	
Unspecified (T4)	Information, software and equipment must be available to the best of our ability	
Associated protective measures and rules shall be developed for the information and the components classified as *Very Critical or Critical*.		

4.4.2.3 Integrity

The following *Integrity classes* are used for the information at Quark Software Inc:

Integrity	Meaning	Examples
Very sensitive to changes (R1)	Incorrect, incomplete or outdated information causes very serious consequences for Quark Software Inc, that in most cases cannot be recovered	• Program code • Files • Databases • File transfer • Parameter settings • Logs
Sensitive to changes (R2)	Incorrect, incomplete or outdated information causes serious consequences for Quark Software Inc but can often be compensated for or adjusted afterwards.	
Less sensitive to changes (R3)	Incorrect, incomplete or outdated information causes only minor or no consequences for Quark Software Inc. Possible errors will most likely be detected.	

4.4.3 Information classification matrix

Allowed combinations of information access depending on approved access type

Rules:

- Remote access is only allowed with Quark Software Inc approved computers.
- Computers shall have updated antivirus and spyware protection.
- Computers shall have personal firewall configured to block all incoming traffic

Location Info class	Open information S4	Intercompany information S3	Confidential information S2	Strictly confidential information S1
Quark Software Inc LAN cable	X	X	X	X
Remote Quark Software Inc PC Internet w/Quark Software Inc Desktop	X	X	X[1]	X[1]
Removable devices (CD's, DVD's, Flash drives, USB tokens, portables drive)	X	X	X[2]	X[2]
Remote Smartphone Internet	X[3]	X[3]	X[3]	
Remote Internet suppliers	X[3]	X[3]	X[3]	

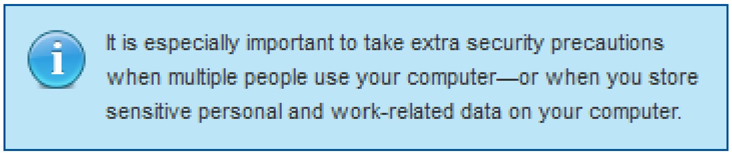
1) Only with hard disk encryption
2) Only with encrypted device
3) Only mail

4.4.4 Employee Acceptable Use Policy

For security and network maintenance purposes, authorized individuals within Quark Software Inc. may monitor equipment, systems and network traffic at any time.

Computer and electronic equipment issued is the responsibility of the User to maintain in good condition, limit damage or loss, and report problems immediately to the IT Department. The IT department will evaluate damage or loss to determine the cause and who is responsible for repairs or replacement.

Quark Software Inc. Business Protection Agreements, Employment Contracts and policies on Security and Proprietary Information apply to this Acceptable Use Policy.



It is especially important to take extra security precautions when multiple people use your computer—or when you store sensitive personal and work-related data on your computer.

Security and Proprietary Information

The user interface for information contained on Internet/Intranet/Extranet-related systems will be classified as either confidential/secure or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.

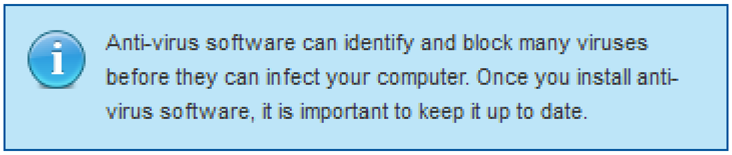
All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended. Auto locking features can be used while away from the computer; “sleep or screensaver” mode will be used on Apple devices.

Postings by employees from a Quark Software Inc. email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Quark Software Inc., unless the posting is in the course of normal business related responsibilities.

All hosts/devices used by the user that are connected to the Quark Software Inc. Internet/Intranet/Extranet, whether owned by the user or Quark Software Inc., shall be continually executing approved virus-scanning software with a current virus database unless overridden by IT.

Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or malware.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Quark Software Inc. trademarks, logos and any other Quark Software Inc. intellectual property may also not be used in connection with any non-work-related activity.



Anti-virus software can identify and block many viruses before they can infect your computer. Once you install anti-virus software, it is important to keep it up to date.

5. Information access control

5.1 *General*

Access control is about preventing the ability to read, change or delete information without being authorized to do so. This is achieved by controlling who gets access to what information by different access controls.

Access controls shall be established for:

- Information that is used and stored in Quark Software Inc’s IT environment, e.g. data files, application information, parameters and configurations. See chapter 5.3, IT environment access control.
- Information that is used and kept outside the IT environment, e.g. paper documents, printed overhead slides and microfiche. See chapter 5.4, Access control of paper-based information.

5.2 *Responsibility*

The *IT Manager* is responsible for appointing resources to implement access controls.

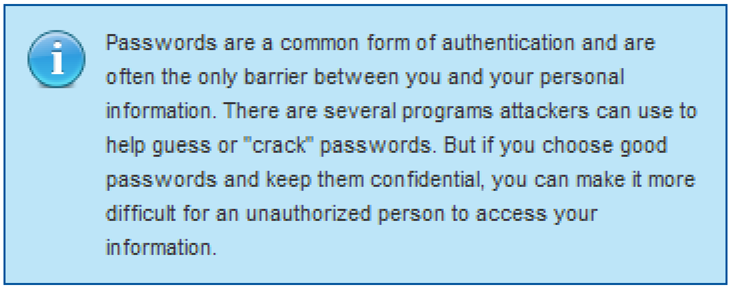
The *information owner* is responsible for all parts of the information security i.e. availability and protection against unauthorized access or modification. The information owner approves access/access levels to the information he/she is responsible for.

The *function owner* is responsible for allot user accounts and access levels to the systems/applications that are used within the function, in accordance with the information owner’s requirement, the basic security level described in this handbook and other requirements such as accountability. Within the responsibility is also to establish suitable access profiles in the IT system on the basis of the employee’s work tasks.

Internal IT is responsible for creating and changing user accounts after approval by the function owner or closest manager (depending on authority level type). Internal IT is also responsible for developing and setting up routines.

Each manager is responsible for informing personnel changes to Internal IT, who will then deactivate access when employment is terminated or evaluate and adjust user access levels when work tasks are changed.

The employee is responsible for protecting his/hers user account and password according to the rules described in chapter 3 Employee’s guide to Information Security.



Passwords are a common form of authentication and are often the only barrier between you and your personal information. There are several programs attackers can use to help guess or "crack" passwords. But if you choose good passwords and keep them confidential, you can make it more difficult for an unauthorized person to access your information.

5.3 IT environment access control

All access to the IT environment shall be controlled by three main access controls:

Access control	Purpose
Identity management (See 5.3.1)	To ensure that only authorized employees have access to specific information the user account shall be approved before given access to the user. The access rights of the user account shall always be based on the employee's current work tasks.
Access control system (See 5.3.2)	The Access Control System shall protect all systems, applications and components with access or connection to critical or sensitive information. Before being logged in to a user account each valid user must be verified with a unique password
Logging and follow-up (See 5.3.3)	To ensure that only authorized employees have access to specific information the existing user accounts and access rights shall be followed-up. This can be achieved by log analysis.

5.3.1 Identity management

Identity management refers to routines to define, approve, register, change and remove user's authorizations and access rights. The routine must guarantee that:

- Each user account is approved before registered.
- The user account access rights are based on the user's actual work tasks.
- Each user is given a personal and unique user account.
- The user account details and password are distributed without risk of ending up in wrong hands. For locked accounts and users asking for new passwords the identity of the user shall be verified.
- A user's access rights are changed when the user is changing work tasks or by other reasons doesn't need the previous access level.
- The user account is removed when the employee is terminating his employment.
- The user accounts for consultants or temporary personnel have a time limit according to the length of the assignment.
- The naming of the user accounts applies to a certain standard to simplify the follow-up of accounts.

Overall there are two main types of access levels:

Access level	Including	Approved by

Standard access	Access rights normally assigned to all users, e.g. network and e-mail accounts, Intranet, the file server of the function or department etc.	Closest Manager
Administrator / operator access	Privileged access rights, which gives the rights to alter system configuration, applications, databases etc. Is assigned to appointed system administrators only.	IT manager/ Functional owner

Privileged access rights mean the right that makes it possible to alter configuration in an application, system or network equipment, create or change user's access rights etc. Privileged access rights shall only be assigned to employees with responsibility to perform such tasks.

Internal IT provides a central function for user account administration and is the function owner of the process. A central register of all actual user accounts and access rights shall be established, ensuring a good control of users and their access rights. Follow-up of access rights can then be performed effectively. The actual request for adding a new user account shall also be archived.

Responsible manager shall inform Internal IT about any personnel changes or changes in assignments for employees, so that the user account or access rights can be changed accordingly. Before the change takes place Internal IT shall inform the actual user and ask for a confirmation from the user's closest manager.

5.3.2 Access Control System

An Access Control System (ACS), to prevent unauthorized access, shall protect all IT systems and resources within Quark Software Inc supporting several users.

Quark Software Inc uses Active Directory (AD) in conjunction for user control on the Windows machines.

The IT department owns the ACS that controls the standard access and access to the infrastructure.

The access control system shall:

- Verify the validity of each user at login.
- Manage the current rules for user accounts and passwords (see below).
- Store and submit passwords in an encrypted format (systems that cannot handle encrypted format must be identified and may get exempted).
- Enable logging (see chapter 5.3.3, Logging and follow-up).

General rules for a user account are:

- The user account is personal and unique. Group accounts are only used if it is necessary and if accountability to a specific employee isn't important.
- Standardized user identities shall be used in order to easily identify the user who holds the account.
- The user account use shall be time limited for temporary users (e.g. consultants).
- Number of login attempts to a user account shall be limited to three (3). If the number of attempts exceeds the limit, then the account shall be deactivated for use. Internal IT can only activate the account again after identification of the user.

General rules for a user password are:

- The password shall consist of at least twelve (12) characters, of which at least two shall be letters and two non-letters.
- When a user has forgotten the password or is locked out from the account a new temporary password shall be created.
- Change of password is requested automatically at first login if the password has been supplied to the user (e.g. for a new employee).
- Change of password is requested automatically by the system at least every 90 days, both for user accounts and privileged accounts.
- The password shall never be shown on the screen
- Systems delivered passwords must be changed directly when installed.
- A password cannot be reused until 5 changes have been made since it was last used.

5.3.3 Logging and follow-up

System logging shall be activated on all IT systems to be able to trace each user's access. The purpose of the logging and follow-up is to:

- Guarantee that the users using the information are still authorized and employed by Quark Software Inc.
- Identify unusual patterns, e.g. several numbers of failed login attempts. This could be an indication of that an unauthorized person has tried to access the information.
- In case of an incident, be able to identify the course of events, actions that are taken and by who the actions were taken.

Only appointed administrators may perform log reviews, where individual user's logins can be traced. The function owner approves authorized administrators.

All users shall be aware of that a log review is performed, which also serves as a preventing measure. (It should be emphasized that this review does not include trace/review of other type of information that belongs to the user. Only the CIO can demand such a trace). The IT department is responsible for establishing the routines for follow-up of logs and for implementing suitable tools.

The log shall at least register the following information:

- User identity, computer/IP address, access request and time.
- Successful and failed login attempts.
- All activities performed by system administrator.

The logs shall be protected from unauthorized access and manipulation. The logs shall be stored during the time necessary based on business or legal requirements. It is the duty of the function owner to survey and define these requirements. When there is a suspicion or confirmation of an incident, this shall be handled according to Quark Software Inc's routines for incidents (see chapter 10). The ISO shall also be contacted immediately.

The function owner shall guarantee that the follow-up is made for existing user accounts and access rights to make sure that they are correct and current, at least once every year. Before any change of access rights or termination of a user account a confirmation shall be received from the user's manager. When the change is made the user shall be informed.

5.3.3.1 Follow-up of outsourced systems and applications

Follow-ups of outsourced systems and applications are equally important. In this case Quark Software Inc personnel will most likely not have the same access to review relevant access control related information and instead have to rely on reports from the third-party vendor.

The function owner shall guarantee that access control reports are collected from the third party on a bi-annual basis.

5.3.4 Remote Access

Remote access users that are connected to Quark Software Inc.'s network via public or other networks must use the VPN solution provided by Quark Software Inc.

5.3.5 Protection of stored information

All information on computers used for remote access must be encrypted when stored, see 4.4.3. The technique for encryption shall be common and approved by the ISO.

5.4 Access control of paper-based information

The person responsible for the information, i.e. the information owner, shall approve access to paper-based information. When the information is stored in a locally allocated and secured room, a register shall be held over the employees having access rights to the room. The receiver shall be informed about how he/she shall store and handle the information in a secure way.

How information shall be protected in different situations, e.g. when distributed or stored, is further described in chapter *3.3 How to protect confidential information.*

6. System, communications and network security

6.1 General

This chapter describes the basic level of security for the IT systems, networks and network equipment that handle Quark Software Inc company information. The purpose is to make sure that the information is kept confidential, available and correct and also to prevent accessibility and availability problems for Quark Software Inc's network and communication environment. The rules for the company's connections to and from public networks such as the Internet are also described.

6.2 Responsibility

The *ISO* has the overall responsibility for Quark Software Inc's IT security organization, system security and network security environment. He shall organize and create opportunities for the introduction of the basic level of security as stated in the information security handbook and defined by the function owner's requirements.

The *IT manager* is responsible for management of the IT and network environment.

The *function owner* is the overall responsible for fulfilling requirements defined by the information owner and rules defined in this handbook

The *technical owner* is responsible for the realization and observance of the systems and network from the function owner requirements and from the basic level of security that is described in this handbook. The technical owner handles the daily operation of the systems and networks at Quark Software Inc. The technical owner shall also report system- or functional faults and incidents that are a threat to the information security.

6.3 General basic level of security for the system- and network environment

Quark Software Inc's system and network environment shall be designed so that the production environment is separated, not necessarily segmented, from the development and test environments. This is to minimize the risks for unauthorized access to the production systems, and to prevent unwanted changes of information in the systems used for production.

Business critical systems that manage information that are classified according to one of the information classes S1, S2, T1, T2, T3 and networks that connect to business critical systems, shall be operational according to 8.5, *Physical protection in a server room*.

The ISO shall approve the IT platforms and shall approve any deviations including assessments of deviations and its security aspects, before they are introduced in the IT environment.

The rules regarding the system and applications security shall be applicable for all programs and hardware that connects to, work or store common information at Quark Software Inc. The rules shall also be applicable for programs and hardware that manage information that is in any way critical or sensitive for the business. This also applies to workstations.

6.4 *Public networks and the Internet*

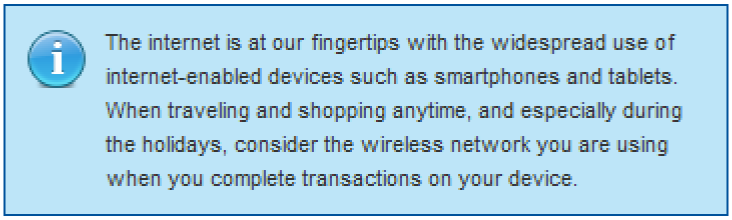
All connections from LAN’s that are used at Quark Software Inc, to Quark Software Inc business critical systems and networks, shall apply to a common solution, which is approved by the ISO.

Public networks are defined as networks where communication with external companies is possible, for example Internet. This means that all communication outside the Quark Software Inc company LAN’s is public. All communication with public networks shall follow a common standard approved by the ISO.

Connections to public network shall be made based on an approved standard. There shall only be approved connections to public networks. All strictly confidential and confidential information that are sent via public networks or the Internet shall be encrypted, with an approved encryption technology, to prevent unauthorized monitoring or change.

All systems that are connected directly to the Internet or are accessible directly from the Internet shall be separated from the internal network. The solution shall make it possible for so called secure networks, DMZ (demilitarized zone), to protect systems that need to be accessed from the Internet (for example Web servers, DNS and external email servers).

External instant messaging is prohibited.



The internet is at our fingertips with the widespread use of internet-enabled devices such as smartphones and tablets. When traveling and shopping anytime, and especially during the holidays, consider the wireless network you are using when you complete transactions on your device.

6.4.1 Firewalls and filtering

All information to and from public networks and the Internet shall be sent via a firewall. The security solution shall support packet filtering of communication making it possible to block traffic with respect to sender- or receiver address, protocol type and port number.

The firewall shall only allow traffic that is necessary for Quark Software Inc’s business operation, which means that all other traffic shall be filtered out. The ISO shall approve the traffic that is allowed to pass through the firewall according to predefined rules. The services shall be evaluated with regard to security. Services that reduce the security level shall, as a general rule, never be used.

The solution shall make it possible to hide the internal network addresses towards the public network.

The rules for filtering are valid also for the outgoing traffic. The solution shall therefore support a secure use of the Internet and prevent the use of performance demanding services.

Traffic and firewalls shall be monitored and logged.

6.5 *Wireless network*

The use of wireless networks inside the Quark Software Inc environment is for Quark employees only within a secured environment.

Using the Quark Software Inc WLAN is equivalent to using any other Quark Software Inc network segment and the same restrictions regarding information confidentiality applies.

All access points shall be reported in advance to the IT department at Quark Software Inc and all instructions regarding channels etc. must be complied.

There shall be documented operational procedures for the WLAN at Quark Software Inc and routines for handling and administration of the clients that will be connected to these networks. This shall include routines for administration in connection with installation, reinstallation, reparation and measures taken in case of loss or theft. These procedures must include the following basic rules:

- All WLAN related equipment used must be Wi-Fi CERTIFIED™.
- Encryption must be used. All installations must use the WPA2-PSK / Enterprise protocol.
- Encryption keys shall, if acceptable routines exist or the standard allows it, be changed regularly.

6.6 Communication solution for remote access

A common and uniform communication solution for Quark Software Inc's personnel shall be used to connect remote access users to Quark Software Inc production system and LAN. This solution shall be based on encrypted communication. The ISO shall approve this solution.

The communication solution shall safeguard that strictly confidential or confidential information can be exchanged in a secure and unchanged way. Secure identification and verification of remote users shall be applied according to the approved standard. The choice of security solution shall be based on an investigation regarding the risks that exists at the employee's work place. The ISO shall approve this solution.

6.6.1 Remote access solution

Remote access users that are connected to Quark Software Inc's network via public or other networks must use the VPN solution provided by Quark Software Inc.

6.7 Operation and maintenance

6.7.1 Change management

There shall be procedures and rules for managing changes in the system and network environment. All change management in the production environment shall be performed according to an approved procedure at Quark Software Inc.

All changes that are made shall be investigated, carefully planned, controlled and approved, based on predefined acceptance criteria, before they are implemented. Changes that are judged to affect information security shall be tested in a separate test environment before they are implemented in the production environment. Changes shall be implemented in a way that they are not negatively affecting the daily business. If an interruption is necessary for implementing the change, then all affected shall be informed.

Implemented changes shall be documented in a logbook or equivalent. The function owner is responsible for updating the documentation with the implemented changes done.

6.7.2 Emergency changes

Emergency changes are defined as an unplanned activity to correct any form of operational disruption in the production environment. When a serious operational disruptions occur, it is often required that actions are taken immediately, which might mean that approved procedures for change management cannot be followed. The emergency changes shall be documented and, after the change has been implemented, be followed up according to the procedures for change management.

All emergency changes in the production environment shall be done according to an approved procedure at Quark Software Inc.

6.7.3 Security upgrades

Security upgrades from vendors make sure that known security weaknesses in systems and applications are handled. For certain systems these upgrades are collected in a larger upgrade packet. These upgrades / packets shall be controlled or analyzed before they are installed in Quark Software Inc's productions environment, to ensure that the operations are not affected negatively.

6.8 Configuration

All IT systems and network equipment within Quark Software Inc shall be configured according to an approved and secure standard configuration. Configurations shall be analyzed with regards to the IT security aspect, to ensure the configuration. The ISO shall approve the configuration standards.

The basic level of security for Quark Software Inc's productions environment includes the following:

- The information owner and the function owner security requirements shall be supported by the configuration.
- Legal requirements or legally binding requirements must be obeyed.
- The IT manager must approve changes, exceptions or deviation from the approved configuration.
- The configuration shall only support connections to approved networks.
- Installation and operational documentation must exist.

6.8.1 Workstations and laptops

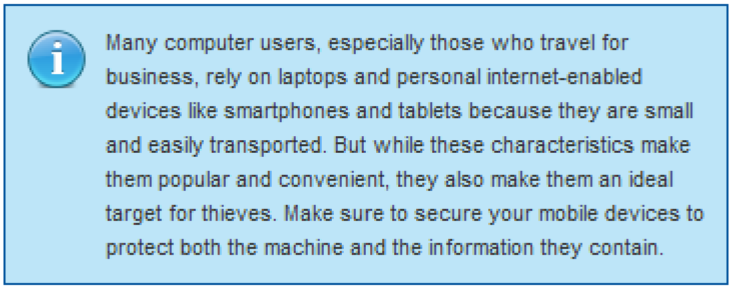
The basic level of security applies to workstations and laptops.

Workstations and laptops shall conform to:

- It is not allowed to use a non-company laptop at work or connect a non-company computer from outside Quark Software Inc's Physical premises to Quark Software Inc's network without approval. The ISO shall approve any deviations.
- Password protected screensavers shall be used on all workstations and laptops. This prevents visitors, among others, to gain access to Quark Software Inc's network.
- Standard password on predefined user accounts shall be changed. Alternatively, if no specific need exits, the user account shall be terminated.

Laptops shall also conform to:

- All laptops shall be marked with an anti-theft label.
- Laptops are not to be left unattended in for example cars, during travels or at public places.
- At work, laptops shall be locked with approved security system when they are not used. The IT Department gives recommendations on approved locking systems.



Many computer users, especially those who travel for business, rely on laptops and personal internet-enabled devices like smartphones and tablets because they are small and easily transported. But while these characteristics make them popular and convenient, they also make them an ideal target for thieves. Make sure to secure your mobile devices to protect both the machine and the information they contain.

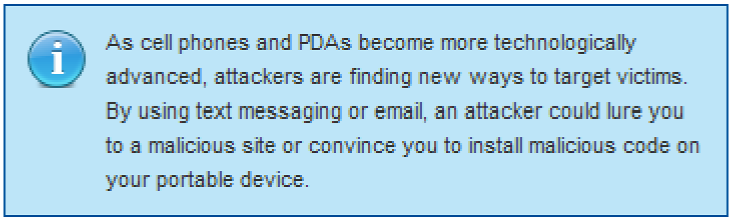
6.8.2 Mobile phones and handheld devices

The basic level of security applies to workstations and laptops.

Mobile phones and handheld devices shall conform to:

- Mobile phones should not be used for storage of any confidential information.
- A screen lock must be implemented to require a password or code to be entered after being idle for 2 minutes or more
- Must not use the default passwords provided by their phone or voicemail service, but must create a new one
- Mobile phones that store or transmit confidential information must have the proper protection mechanisms installed, including antivirus software. All unneeded services and ports must be turned off and applications must be properly configured.

  These mechanisms are the required compensating controls referred in section 7.
- Mobile phones which cannot use encryption because of technology limitation but have compensating controls may be granted special waiver. However, these systems and applications must still be thoroughly risk assessed to ensure that major risks are addressed via compensating controls to protect the data in lieu of not using encryption
- In addition to the items outlined above, an individual who is given a phone owned by Quark Software Inc, agrees to the following:
  - They will report any loss or theft of their phone or mobile device to management within 24 hours.
  - They consent to having their phone's or mobile device's data wiped in the event of loss or theft to protect any data stored on the device.
  - They agree to abide by best practices as outlined in this and other technology policies, which can be amended by management at any time.
  - At contract termination phones and mobile devices shall be reset using factory reset to wipe all data from the mobile device.



As cell phones and PDAs become more technologically advanced, attackers are finding new ways to target victims. By using text messaging or email, an attacker could lure you to a malicious site or convince you to install malicious code on your portable device.

6.9 Monitoring and logging

Network activities shall be monitored and logged in order to discover security related deviations or abuse. This is valid for all incoming and outgoing traffic through the firewall and all configuration changes. Appointed and responsible administrators shall analyze the logs regularly. The log shall, if possible, contain the following information:

- Time (Year, Month, Day, Time)
- Identity (User identity, IP address or similar)
- Service
- Port.

The logs shall be saved according to requirements identified in a risk analysis and according to Quark Software Inc's requirements (for example as evidence in a trial). The logs shall be protected from unauthorized access and manipulation. An alarm shall be issued to the administrator at the following incidents:

- The firewall is getting close the set limit values (capacity, simultaneous calls, etc.). The limit values shall be documented.

7. System development and procurement of standard systems

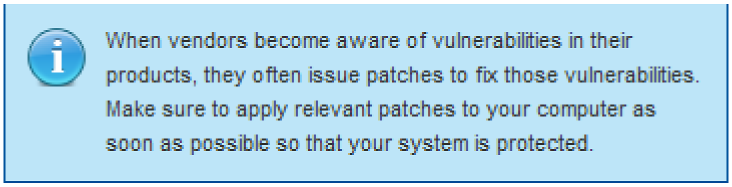
7.1 General

This chapter describes the basic level of security on how information security shall be included in the system development process or during procurement of a standard system within Quark Software Inc. Risk analysis shall be performed in order to define necessary requirements for the system. The security requirements are governing for the system; regardless of it is a system that is developed by Quark Software Inc, developed externally or standard system procured from an external company.

7.2 Responsibilities

The *information owner* is responsible for the information that is managed in the system and is responsible for defining requirements to the function owner regarding information security.

The *function owner* is often the requestor of the system and defines the requirements on the system regarding functionality and security. The function owner is responsible for the security of the system and that updates are installed according to the approved procedures. This responsibility includes taking measures to reduce the external risks identified in the risk analysis.



When vendors become aware of vulnerabilities in their products, they often issue patches to fix those vulnerabilities. Make sure to apply relevant patches to your computer as soon as possible so that your system is protected.

The *project leader* is responsible for informing the project members regarding the information security rules during the project, and that the project abides to the security rules during system development. The project leader is responsible for carrying out risk analysis and test software according to Quark Software Inc's security requirements.

The *project members* are responsible for checking that their work follows the procedures defined by the project leader and the security rules that are approved at Quark Software Inc.

7.3 Security in a development project

During a system development project all systems and software shall be protected in the same way as the finished products. Suitable measures shall be applied to protect the specification of requirement and other specifications from un-authorized access.

This also includes the source code for the systems and software that are being developed, i.e. that the users access to the archives for the source code is controlled in a secure way.

The development- and test environment shall also be separated from the production environment.

7.3.1 Change management and version control

Rules and procedures for change management and version control shall be used in the project. This is to make sure that traceability between different versions in a development project exists, that is from the latest software release back to earliest releases.

The project leader is responsible for ensuring that the rules used for the system- and program changes are used and to inform the other project members about the rules. It shall also be possible to trace the changes in the code regarding who has done a change, time of change and reason for the change.

The project leader shall approve all changes before they are implemented.

7.3.2 Definition of security requirements

The security requirements shall be defined for each system based on a risk analysis. Risk analysis shall include the system, its information and requirements according to the current laws and regulations. The security requirements on the system shall clearly be documented in the specification of requirements for the system.

7.3.3 Models for project steering and system development

A documented method for project steering and system development shall exist at Quark Software Inc. All development of business-critical systems and application that handles information classified with any of the information classes S1, S2, T1, T2 or T3 shall follow this approved model.

7.3.4 Verification

Critical information that is being handled by IT systems or applications shall automatically be verified to minimize the risk of errors. These controls shall be built in to the system ensuring that the information has not been modified, due to erroneous processing or incorrect inputs (for instance abnormally high values or a large number of characters). By doing these verification checks in the system most of the common security problems such as buffer overflows, are prevented.

The need for confidentiality shall be considered with regards to the value of the information and the current model for information classification. All together the appropriate verification is chosen in such a way that the security requirements are meet. See chapter 4.4 regarding Information classification.

7.3.5 Guidelines for testing and quality assurance

The integrity of the output shall be verified during the test phase by automatic validity controls. These controls can also be extended if needed with manual controls.

Data that are used in system- and acceptance tests shall be as similar as production data as possible, but test on production data shall be avoided if possible. The ISO and personal data controller shall approve personal data that are needed in the tests, and all information regarding persons shall be removed making it impossible to trace whose personal data those are. The test data shall also be protected according to:

- Operational procedures that are used for controlling access to the production environment shall be used during the tests.
- Special authorization shall be given every time information classified as S1 or S2 is copied from the production environment to the test environment.

- Data from the production environment shall be erased from the test system after the tests are concluded in a safe manner.

Before any new or modified systems or applications are made operational, they shall be acceptance tested in an environment that is separated from the production environment. The buyer/function owner shall formally approve the system after the acceptance tests are concluded.

7.3.6 Guidelines for implementing a project in production

This procedure shall contain a description of the procedures and rules that needs to be followed when a system is moved from the development environment to the production environment. The approved rules for approving a system for operations and handing over shall be applied before each new system is made operational. The necessary system- and operational documentation shall exist when the handover is made. It is the responsibility of the project to develop this documentation.

7.4 Outsourcing of the system development to an external company

When the system development is outsourced to an external company a formal agreement shall be drawn up. The agreement shall at least contain the following:

- The responsibility on Quark Software Inc and on the external company.
- The responsible contact persons at the external company.
- The authorization for the external company and access rights during the project.
- Requirements on the system- and user documentation.
- License issues.
- Owner and immaterial rights to the source code and the finished product.
- Deposit of the source code in the case the external company is not able to conclude the agreement.
- Tests before installation.
- Fines if the external company does not fulfill the requirements according to the agreement.
- Confidentiality agreement for all consultants that will be involved in the development project.
- Quality requirements on the source code.
- The conclusion of the project and the delivery of the final product.

When the assignment is finished all access right to Quark Software Inc’s system shall be revoked. The external company shall hand over all information and software to Quark Software Inc, if not stated otherwise in the agreement. The function owner is responsible for the above statements.

7.5 Security when procuring a standard system

The security requirements shall be defined before ordering a standard system, for example from a risk analysis (see chapter 4.3). The security requirements shall be clearly stated in the system requirement specification.

The goal when procuring a standard system is that all security requirements shall be met. In the cases where the standard system does not comply with the requirements, then all requirements that are not met shall be documented. It shall be investigated if unfulfilled requirements can be reached in any other way, for example by the help of compensating controls or tools.

For each standard system a formal agreement shall be drawn up with the supplier. The agreement shall at least contain the following, where applicable

- The responsibility of Quark Software Inc and of the supplier
- Requirements regarding documentation.
- The number of licenses bought.
- Support agreements including appearance time and time to completion.
- Fines if the supplier does not fulfill the agreement.
- Confidentiality agreement with the supplier.
- Upgrade procedures for the system.
- Security requirements on the standard system according to the requirement specification.
- Training of personnel.
- Fulfillment of legal requirements.
- An escrow agreement securing access to the source code in case of insolvency of the supplier.

The ISO shall approve all procurement of standard systems for Quark Software Inc.

7.5.1 Requirements on the supplier of standard systems

The financial stability of the supplier shall be checked. An assessment shall be done if there is a risk that the supplier will become insolvent or close down. If this is risk, it can result in that the system cannot be delivered or maintained. The supplier shall supply all necessary documentation. The supplier should have a test environment where Quark Software Inc's security requirements can be verified.

7.5.2 Adaptation of a standard system

Standard systems shall, as far as possible, be used without being modified or changed. An analysis shall be made on the effect on the security of the system and the operational environment prior to making any adaptations. There shall be an investigation made on how changes affect the agreement with the system supplier, for example the responsibility for unforeseen faults that are caused by the changes. This shall be done in cooperation with the supplier. All adaptations that are done in the system shall be documented and enclosed the system documentation.

7.5.3 Guidelines for introducing a system in production

The same rules apply for introducing a standard system in production as for introducing a system that has been developed by Quark Software Inc (see chapter 7.3.6). All predefined user accounts shall be removed if they are not specifically needed. The supplier shall supply information regarding the predefined user accounts.

7.6 Redundancy

The project is responsible for investigating if there shall be any redundant software or hardware to fulfill the availability requirements that the function owner has defined. The function owner in cooperation with the technical owner shall make the investigation. The suggested solution shall be approved by the function owner.

7.7 Documentation

Detailed system, user and operational documentation shall be produced by the development project. The supplier shall produce the documentation for a standard system. A responsible person shall be appointed that is responsible for making sure that the documentation is updated and current. The documentation shall be classified. Confidential documentation shall be handled with regards to the current handling rules. The procedures shall safeguard that the documentation is updated when changes are introduced.

8. Physical security for information and IT systems

8.1 General

This chapter describes the rules on Physical protection for information, IT systems and critical network equipment. The chapter does not describe other Physical security such as security for personnel, building as a whole or property. The chapter is divided in the following parts:

- General security rules for server rooms.
- Physical protection in server rooms.
- Physical protection for written documents.

A server room is defined as a normal room that has been reserved for IT equipment.

Equipment that needs to be accessible by the employees of Quark Software Inc, for instance printers, copy machines or paper materials, are not allowed to be placed in a server room.

All cross-connection racks (for data and telephony) shall have a reasonable Physical protection. *Access to the racks is controlled by the IT department.*

8.2 Responsibility

The ISO is responsible for the Physical security within Quark Software Inc. Included in this responsibility is the task to create opportunities for Physical protection according to this chapter.

8.3 General rules for server rooms

The following general rules are valid for server rooms:

- Only authorized personnel shall have Physical access to server rooms.
- Authorized personnel are defined as persons that need to have Physical access to be able carry out their work.
- It is not allowed to eat, drink or smoke in a server room.
- All photography, video, sound or other recording is forbidden unless the ISO has granted a special permit.

8.3.1 Housekeeping

All authorized personnel are responsible for keeping the server room in good order.

- Servers and other communication equipment shall be placed in special cabinets or server racks.
- Server rooms shall, under no circumstances, act as storage space. Only necessary equipment and necessary manuals are allowed. This means for instance that printers, generally accessible by Quark Software Inc employees, shall not to be placed in a server room.

- The removal of packing material shall be done outside the server room to protect the equipment from dust particles or unnecessary and fire hazardous material.

8.3.2 Replacing equipment

When replacing old equipment with new, hard drives and other storage media shall be destroyed. All destruction (independent of method) shall be done outside server rooms. In the case where an external company is hired to collect and destroy the equipment it shall be included in the agreement that the data shall not be possible to recreate after the destruction is done. The external company shall also sign a confidentiality agreement.

8.4 Physical protection in server rooms

8.4.1 Access protection

The server room shall have an approved door with an approved lock. The door shall at all times be locked. Access to the server room shall only be possible for authorized personnel. If keys are used, then they shall be of a copy protected model

Visitors to the server room, for example service personnel, shall wear a badge visual at all time.

Glass windows shall be protected by security glass or by safety cages.

8.4.2 Fire protection

The following fire protection is valid for server rooms:

- The server room shall be equipped with approved and regularly tested fire appliances adapted to the size of the room.
- Hand held fire extinguisher and fire blankets shall be available in sufficient number according to a completed fire safety investigation
- Server rooms shall be equipped with fire detectors. The alarm shall be heard outside the server room.
- The fire escape plan shall be posted on a visible place and be tested regularly.
- The supplier or equivalent should regularly test the fire protection.

8.4.3 Power supply and electrical environment

Availability critical equipment shall have power supplied via an UPS (Uninterruptible Power Supply). It shall be installed according to the supplier’s instructions and be tested regularly.

Power distributors are not allowed to use for equipment in the server room.
.

8.5 Physical protection for paper documents

Original documents, such as contracts, must be protected against damage. Such documents shall be kept in locked cabinets.

Confidential documents, such as construction plans and unpublished annual earnings figures, shall be protected against unauthorized access. Such documents shall be kept in lockable cabinets; to which only authorized personnel has access (see chapter 5 Information access control).

The person who is responsible for Physical security shall consult with the people responsible for such information in order to estimate the needs of safe cabinets or rooms.

Confidential documents shall be destroyed after they have been used.

8.6 Storage

Original documents or documents and data containing highly sensitive information must be protected against unauthorized access and damage:

- The storage must be planned in such a way that confidential information is not exposed to unauthorized access. Original documents shall be kept apart from security copies, in order to prevent both from being destroyed in the event of fire, water damage, explosion or other disastrous events.
- The demand for security classified cabinets or rooms, approved as fire- or burglar proof by the corresponding authority, shall be analyzed at the request of the people responsible for the respective functions.

8.6.1 Clean desk / screen rules

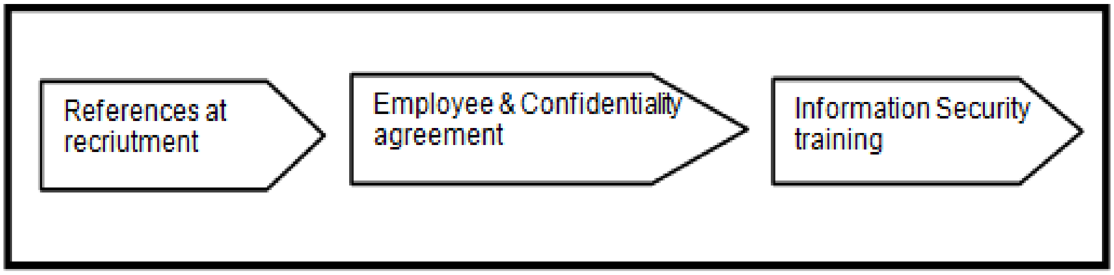
In order to minimize the risks of unauthorized access, loss of and damage to information during and after normal work hours the following rules should be observed:

- Information that is confidential or strictly confidential shall be locked up (preferably in a fire proof cabinet) when it is not needed, especially when a function or unit is left unattended.
- If the authorized person is not at his/her workplace, all paper documents, as well as data storage media labeled as sensitive, must be removed from the desk or other places (printers, fax machines, photocopiers, etc.) to prevent unauthorized access.
- Personal computers, terminals and printers must not be left logged in when they are unattended. Portable or handheld computers shall be locked in when they are not used.
- If the authorized person is not at his/her workplace, all sensitive information must be removed from the screen. The clear screen policy is implemented by logging out of all systems or locking the screen with a password.

9. Information security within personnel management

9.1 General information

This chapter describes the rules that need to be applied within the personnel administration process; recruitment, employment and end of employment. New employees shall be informed of the existing rules of information security and associated Quark Software Inc security handbook.


References at recriutment
Employee & Confidentiality agreement
Information Security training

9.2 Responsibilities within personnel management

The CIO is responsible for ensuring that the company fulfills the rules and requirements established in the policy and the handbook. To summarize, the responsibility includes the following; related to personnel management:

- Allocate resources to ensure that the rules for information security in the handbook get communicated, applied and maintained.
- Ensure that sufficient information security responsibility is established and communicated.

The ISO of the Company has the overall responsibility for and coordination of the IT security at Quark Software Inc. To summarize, the responsibility includes the following; related to personnel management:

- Following up, to ensure that the information security rules and procedures are followed.
- Report serious information security incidents to the company management.
- If necessary give exemptions from policies, guidelines or instructions.
- Being the contact for the information security responsible persons in the company.

The Manager with personnel responsibilities has the following responsibilities;

- Introduce rules of information security in relation to recruitment, employment or end of employment.
- Making information security training being part of the introduction for employees at “Quark Software Inc”.
- Ensuring that the employee has the opportunity to participate in security training.
- That time is allocated for issues regarding information security at the department

meetings.

- Decides on any actions to be taken if rules are broken.
- To ensure that contractors and other external staff within his responsibilities follows the rules in this handbook.

The employee is responsible for applying existing information security rules and taking part in training regarding such issues.

The employee has a responsibility to follow the rules for information security outlined in this handbook. The employee shall in her work always consider what is best for Quark Software Inc. The employee's responsibilities are summarized in *chapter 3 Employee's guide to Information Security.* In short, the responsibility includes the following:

- Protect confidential and strictly confidential information from being accessed by unauthorized people.
- Use e-mail and the Internet for work related purposes only.
- Protect passwords, keys and other equipment used to access the IT environment, buildings or other facilities.
- Report security incidents.

9.3 Information security from recruitment to end of employment

References – During recruitment the Manager with personnel responsibilities shall verify and follow up the references of the applicant. This is done in order to make sure that the applicant is not known to have broken information security rules during his previous employments.

Terms of employment – Terms of employment shall include:

- Commitment to fulfill the requirements of the Information security policy and the rules of the Information security handbook
- Actions to be taken in case of violations of the Information security rules of Quark Software Inc.

Confidentiality Agreement – The employee shall sign a confidentiality agreement regarding the business and any information related to it. The agreement shall clearly indicate that the confidentiality still applies after the employment is ended. Such a confidentiality agreement may be a part of the terms of employment.

Work Description – The responsibilities of the employee regarding security shall be stated clearly. This is particularly important if the role of the employee has explicit responsibilities for information security.

End of employment – When an employee leaves the company, his manager or IT is responsible for collecting material, equipment, keys etc. limiting access to the "Quark Software Inc" premises and IT environment. The responsible manager is responsible for follow the procedures outlined in the Employee/contractor start and termination" document.

9.4 Information security for contractors

Background check – The Manager signing the contract must verify that background checks have been performed for contractors with access to sensitive information as described in the Quark Software Inc procedure "Contractor background check".

Terms of contract – Terms of the contract shall include:

- Commitment to fulfill the requirements of the Information security policy and the rules of the Information security handbook
- Actions to be taken in case of violations of the Information security rules of Quark Software Inc.

Confidentiality Agreement – The contractor shall sign a confidentiality agreement regarding the business and any information related to it. The agreement shall clearly indicate that the confidentiality still applies after the contract ends.

End of contract – When the contract comes to an end, the responsible manager is responsible for collecting material, equipment, keys etc. limiting access to the “Quark Software Inc” premises and IT environment. The responsible manager is responsible for follow the procedures outlined in the Employee/contractor start and termination” document.

9.5 Training

Every employee with access to the IT environment or to any sensitive information shall take part in training regarding existing rules of Information security. Such training may be a part of the introduction course but shall also be offered to existing employees.

The training shall at the least inform the employee of the following things:

- Rules that apply to information security.
- Where to find the Information security policy and the Information security handbook.
- In which way information of new or modified rules is distributed in the company.
- To whom the employee may turn with questions.

After completion of the training the employee should sign a document stating that he or she has been informed of and is willing to accept the rules in the Information security handbook

Training or distribution of information shall be carried out continuously, in order to ensure that the awareness of the employee regarding information security issues is maintained. It should also be considered to have the personnel of the IT department (staff, superiors and security staff) take part in specialized training.

10. Incident handling and reporting

10.1 General Description

This chapter describes how to handle and report incidents that occur regarding sensitive or time crucial information.-

10.2 Responsibility

The ISO is responsible for reporting security incidents related to unauthorized spreading of information. The ISO is also responsible for handling IT related incidents related to business-critical systems and networks.

The IT Manager that manages the infrastructure and networks is responsible for incident handling for those.

The Technical Owners that manages business critical systems are responsible for incident handling for those systems.

Each employee is responsible for reporting to internal IT and his manager immediately if they find or suspect some kind of weakness or incident.

Internal IT is the focal point for handling information security related incidents.

10.3 Incident handling and reporting

There shall be incident handling routines that clearly describe appropriate measures to be taken if an incident is discovered regarding sensitive information or business critical IT systems.

Incident in this context means e.g.:

- Serious disturbance directed towards availability.
- Grave deficiencies regarding the integrity of information.
- Attempted or successful intrusions.
- Economic irregularities.

Incidents shall be classified in different levels according to their consequences and potential damage. Incidents with more far reaching consequences and potential damage shall be given higher priority than other types of incidents. Incidents concerning viruses (or harmful code) must be reported and actions coordinated to prevent other systems and companies being infected.

Incidents shall be reported to the nearest manager and to internal IT, who is responsible for the matter being taken care of.

Internal IT shall register incidents that occur. Such a register shall include time, scenario, systems or units concerned and who discovered the incident.

If there is a system log or equivalent available, then information regarding the course of events shall be saved by the employee who is responsible for the log. The person, who is responsible for the concerned system or unit, shall investigate the incident in order to prevent similar future incidents.

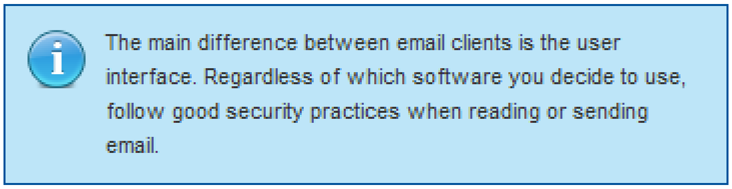
Internal IT shall report serious errors immediately to the ISO. Serious incidents related to IT are also to be reported to the IT Manager. An employee’s Manager shall be informed whenever an incident involves personnel. The Manager or the CIO alone has the right to start an investigation of such an incident. Internal IT shall provide the ISO with continuous reports regarding incidents.

11. E-mail & Social Media Usage

11.1 E-mail use

11.1.1 General description

This policy defines and distinguish acceptable/appropriate from unacceptable/inappropriate use of electronic mail (email). It applies to all users of the Quark Software Inc email system.



The main difference between email clients is the user interface. Regardless of which software you decide to use, follow good security practices when reading or sending email.

11.1.2 Guiding principles

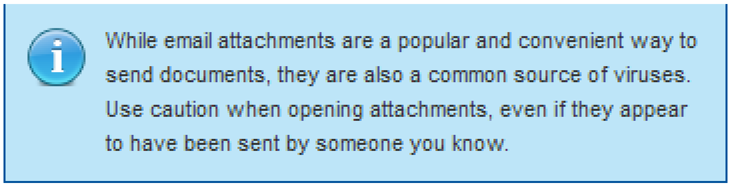
- Email users are responsible for avoiding practices that could compromise information security.
- Corporate email services are provided to serve operational and administrative purposes in connection with the business. All emails processed by the corporate IT systems and networks are considered to be the organization’s property.

11.1.3 Detailed policy requirements

- Apply your professional discretion when using email, for example abiding by the generally accepted rules of email etiquette. Review emails carefully before sending, especially formal communications with external parties.
- Do not unnecessarily disclose potentially sensitive information in “out of office” messages.
- Emails on the corporate IT systems are automatically scanned for malicious software, and spam. Unfortunately, the scanning process is not 100% effective (e.g. compressed and encrypted attachments may not be fully scanned), therefore undesirable/unsavory emails are sometimes delivered to users. Delete such emails or report them as security incidents to internal IT.
- Be vigilant of phishing emails, esp. senders impersonating to be the CEO or some other senior staff member of Quark Software Inc. and asking for your mobile phone number and attempting to seek monetary favors, gift cards or in form of sharing personnel information. Always remember an email originating within the Quark Software Inc. email systems will have the senders profile picture, email signature etc. If it does not seem right, seek IT teams help to determine if a request is legitimate.
- Limited personal use of the corporate email systems is permitted at the discretion of local management provided always that it is incidental and occasional and does not interfere with business. You should have no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees.
- Do not auto-forward corporate email to external/third party email systems. You may access your own webmail via corporate IT facilities at local management discretion provided that such personal use is strictly limited and is not considered private (see previous statement).
- Be reasonable about the number and size of emails you send and save. Periodically clear

out your mailbox, deleting old emails that are no longer required and filing messages that need to be kept under appropriate email folders. See the email retention (11.2) for further details.

- Do not use email:
  - To send confidential/sensitive information, particularly over the Internet,
  - To create, send, forward or store emails with messages or attachments that might be illegal or considered offensive by an ordinary member of the public i.e. sexually explicit, racist, defamatory, abusive, obscene, derogatory, discriminatory, threatening, harassing or otherwise offensive;
  - For private or charity work unconnected with the organization's legitimate business;
  - In ways that could be interpreted as representing or being official public statements on behalf of the organization, unless you are a spokesperson explicitly authorized by management to make such statements;
  - To send a message from anyone else's account or in their name (including the use of false 'From:' addresses). If authorized by the manager, a secretary may send email on the manager's behalf but should sign the email in their own name per pro ('for and on behalf of') the manager;
  - To send any disruptive, offensive, unethical, illegal or otherwise inappropriate matter, including offensive comments about race, gender, color, disability, age, sexual orientation, pornography, terrorism, religious beliefs and practice, political beliefs or national origin, hyperlinks or other references to indecent or patently offensive websites and similar materials, jokes, chain letters, virus warnings and hoaxes, charity requests, viruses or other malicious software;
  - For any other illegal, unethical or unauthorized purpose.



While email attachments are a popular and convenient way to send documents, they are also a common source of viruses. Use caution when opening attachments, even if they appear to have been sent by someone you know.

11.2 E-mail retention

11.2.1 General description

The Quark Software Inc email retention model is to keep mails on remote media for 1 year, no mails in any folder (except Trash, see below) are going to be automatically deleted. However, employees are encouraged to periodically clear out the mailbox and deleting old emails that are no longer required.

Emails containing sensitive information must always be deleted as soon as the information no longer is needed.

11.2.2 Trash retention period

Quark Software Inc email system will be configured to automatically delete messages that have been marked for deletion by users but are still sitting in their "Deleted items/Trash" folders for more than 30 days on active email server.

11.2.3 Litigation holds

When litigation is pending or threatened against Quark Software Inc or its employees, all documents and records that pertain to the issues should be preserved. A litigation hold directive must be issued to the legal custodians of those documents.

A litigation hold directive overrides this email retention policy, as well as any records retention schedules that may have otherwise called for the transfer, disposal or destruction of relevant documents, until the hold has been cleared.

Email and accounts of separated employees that have been placed on litigation hold status must be maintained by the IT department until the hold is released.

No employee who has received a litigation hold directive may alter or delete an electronic record that falls within the scope of that hold. Those employees are required to provide access to or copies of any electronic records that they have downloaded and saved, or moved to some other storage account or device.

11.3 Social Media Use

The following principles apply to professional use of social media on behalf of Quark Software Inc. as well as personal use of social media when referencing Quark Software Inc.

Employees need to know and adhere to the Company's Code of Conduct, Employee Handbook, and other company policies when using social media in reference to Quark Software Inc.

Employees should be aware of the effect their actions may have on their images, as well as Quark Software Inc. image. The information that employees post or publish may be public information that is available for long periods of time.

Employees should be aware that Quark Software Inc. may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to the company, its employees, or customers.

Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.

Employees are not to publish, post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.

Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized Quark Software spokespersons.

If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.

Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.

Social media use shouldn't interfere with employee’s responsibilities at Quark Software. Quark Software Inc. computer systems are to be used for business purposes. When using Quark Software Inc. computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, blogs, LinkedIn and anything else considered publically visible), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.

Subject to applicable law, after-hours online activity that violates the company’s code of conduct or any other company policy may subject an employee to disciplinary action or termination.

If employees publish content after-hours that involves work or subjects associated with Quark Software, a disclaimer should be used, such as this: “The postings on this site are my own and may not represent Quark Software positions, strategies or opinions.”

It is highly recommended that employees keep Quark Software Inc. related social media accounts separate from personal accounts, if practical.

11.4 Avoiding Social Engineering and Phishing attacks

11.4.1 What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, colleague or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

11.4.2 What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

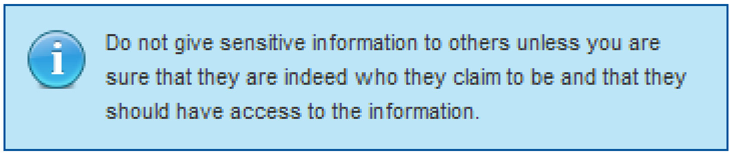
- natural disasters (e.g., Hurricane Katrina)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

11.4.3 How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the internet before checking a website's security.
- Pay attention to the Uniform Resource Locator (URL) of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.
- Take advantage of any anti-phishing features offered by your email client and web browser.

11.4.4 What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including IT administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed.
- Watch for other signs of identity theft.



Do not give sensitive information to others unless you are sure that they are indeed who they claim to be and that they should have access to the information.

12. Encryption

12.1 General description

This policy defines the encryption standards for Quark Software Inc. It provides guidelines to situations for encryption usage. It also provides guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Anyone who accesses, uses, or controls Quark Software Inc electronic information resources should be familiar with this policy.

12.2 Exclusions & special situations

Existing systems and applications containing confidential information which cannot use encryption because of technology limitation but have compensating controls may be granted special waiver. However, these systems and applications must still be thoroughly risk assessed to ensure that major risks are addressed via compensating controls to protect the data in lieu of not using encryption.

12.3 Encryption of Confidential information

Whether information should be encrypted or not, at rest and in transit, depends on the situation and the information classification the information has been assigned. This classification and the proper protection are documented in section 3.3 “How to protect confidential information”.

12.4 Encryption strength

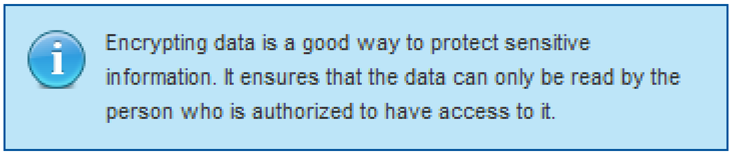
All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit AES.

12.5 Sub-contractors or agents

Any confidential information transmitted to a subcontractor or an agent, or their subcontractors or agents must be encrypted according to **all** of the above standards.

12.6 Key management

- Private keys must be kept confidential
- Short life keys are to be used, ensured by having activation and deactivation dates
- Long-life keys are to be used sparingly
- Keys must be chosen randomly from entire key space
- Keys for encrypting keys must be used separately from keys used for decrypting data. They are not interchangeable



Encrypting data is a good way to protect sensitive information. It ensures that the data can only be read by the person who is authorized to have access to it.

13. Data privacy

13.1 General description

Our data privacy policy sets out our commitment to protect personal data and describe how we implement that commitment with regards to the collection and use of personal data.
We are committed to:

- Ensuring that we comply with the seven data protection principles, as listed below
- Meeting our legal obligations as laid down by the laws in respective country
- Ensuring that data is collected and used fairly and lawfully
- Processing personal data only in order to meet our operational needs or fulfill legal requirements
- Taking steps to ensure that personal data is up to date and accurate
- Providing adequate security measures to protect personal data
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- Ensuring that all staff are made aware of good practice in data protection
- Ensuring that everyone handling personal data knows where to find further guidance

13.2 Data protection principles

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects under the laws in respective country
- Appropriate technical and organizational measures shall be taken against unauthorized and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

14. Compliance and follow-up of Information Security

14.1 General Description

This chapter aims to describe:

- Security awareness – information/ training to make sure the Quark Software Inc personnel is aware of how to act in an appropriate manner when it comes to securing Quark Software Inc and customer sensitive information
- Compliance – Inspection for the purpose of evaluating to what extent Quark Software Inc is fulfilling the Information security policy and handbook as well as handling of any deviations that may occur
- Updating the Information Security Policy and Handbook – Evaluation of the requirement and rules of the Information security policy and handbook in order to ensure that they are up to date and adequate over time.

14.2 Responsibility

The Information Security Officer is responsible for:

- Continuous evaluation of the rules in the policy and the handbook for the purpose of ensuring that they are up to date and adequate over time
- Carrying out various activities aiming to make sure that the Quark Software Inc personnel are fully aware of how to behave with regards to information security.

The IT Manager is responsible for:

- Carrying out inspections for the purpose of evaluating to what extent the IT environment conforms to the Information security policy and the rules of the Information security handbook.

The Internal Audit function is responsible for:

- Performing inspections in order to evaluate to what extent the business activities are adhering to the Information security policy and the rules in the Information security handbook.

14.3 Security awareness

14.3.1 General

All Quark Software Inc personnel shall attend, as a minimum, a yearly information security awareness meeting/training held by the Information security officer. The purpose of this meeting is to update the personnel of existing as well as new information security rules, guidelines, and requirements, to make sure the personnel know how to behave when it comes to information security.

The participation in these meetings shall be noted and any person who fails to participate are instead obliged to read parts of the Information security handbook, pointed out by the ISO, and sign a form of confirmation.

All new Quark Software Inc employees shall be asked to read dedicated parts of the ISH, and to sign a confirmation form.

14.3.2 Incident response

At the annual personnel information security awareness meeting (14.3.1) the ISO shall inform/train the staff how to behave in case of a security incident. This training shall be based on a number of different security incident scenarios and cover actions expected by the employee, escalation procedure, as well as the overall purpose of a quick and correct management of security incidents.

All Directors with in Quark Software Inc with dedicated personnel shall attend a separate information/training meeting with the ISO covering how to act in case of a security incident involving their staff. The training shall be based on a number of different incident scenarios, and cover actions expected by the director, and escalation procedure.

The Quark Software Inc IT personnel shall attend a yearly meeting with the ISO covering the management of information security incidents from an IT perspective. The training shall be based on a number of different incident scenarios, and cover actions expected by the IT personnel, as well as escalation procedure.

14.4 Compliance

The *Internal Audit function* shall see to that inspections are carried out as to what extent the business activities conform to the Information security policy and the rules of this handbook. Any weakness that may be identified upon inspection shall be planned for and handled by the corresponding person in charge.-

In order to evaluate the IT security level, analyses directed towards IT security shall be carried out to support the evaluation of the compliance of the Information security handbook. In case of any security incidents, which supposedly originated from an IT system, an inspection of the technical protection must be undertaken immediately.

Employees who violate the rules of the Information security policy and handbook shall be given sufficient information or training to guide the employee towards a correct behavior and may result in dismissal for multiple offenses.

14.5 Deviations

The Information security officer shall approve any deviations from the Information security policy or the rules of this handbook. Applications for deviations must be in writing and include descriptions of:

- The reason for the deviation.
- Risk and consequences due to the deviation.
- Action plan to make it possible to follow the rule.

14.6 Remediation

The results of any self-, internal-, external- audit should be presented to the senior management and the ISO of the company.

The ISO is responsible for initiating the creation of, and managing execution of, a remediation plan for the identified risks and issues.

14.7 Updating the Information Security Policy and handbook

The rules of this Information security handbook shall be evaluated periodically to ensure that they are up to date and complete with regard to the present situation of Quark Software Inc. The Information security officer is responsible for necessary updates being made.

The information security and the basic level of protection are affected by both business internal and external factors:

- Existing as well as new security risks in the business must be mapped out to ensure that the security level is sufficient.
- Changes to the information security requirements.

The surrounding world must be taken into account. The development within the IT area brings about new possibilities but also new threats to the business. New or modified legislation regarding information security, business requirements etc. must be captured and the information handling adjusted in consequence.

15. Appendix A. (List of Policies)

The below list of additional more specific policies available on Box under:

All Files > Information Security Policies (Published)

- Acceptable Use Policy
- Access Review Procedures
- Access Control Policy Cloud_EN_1.1
- Antimalware Policy
- Data Encryption Policy
- Firewall Router Configuration Standard
- Incident Response Policy
- Information Security Program
- Security Awareness and Training Policy
- System Development Lifecycle
- Vendor Management Policy

- Docurated_v2 – Application Security Standard
- Docurated_v2 - Business Continuity Policy
- Docurated_v2 - Data Classification and Handling Policy
- Docurated_v2 - Disaster Recovery Policy
- Docurated_v2 - Log Management Policy
- Docurated_v2 - Log Management Review Procedures
- Docurated_v2 - Network Security Policy
- Docurated_v2 - Patch Management Policy
- Docurated_v2 - Physical Access Policy
- Docurated_v2 - Risk Management Policy

16. Acknowledge and Acceptance

Full Name	
Acknowledge & Accept	I Accept

Submit