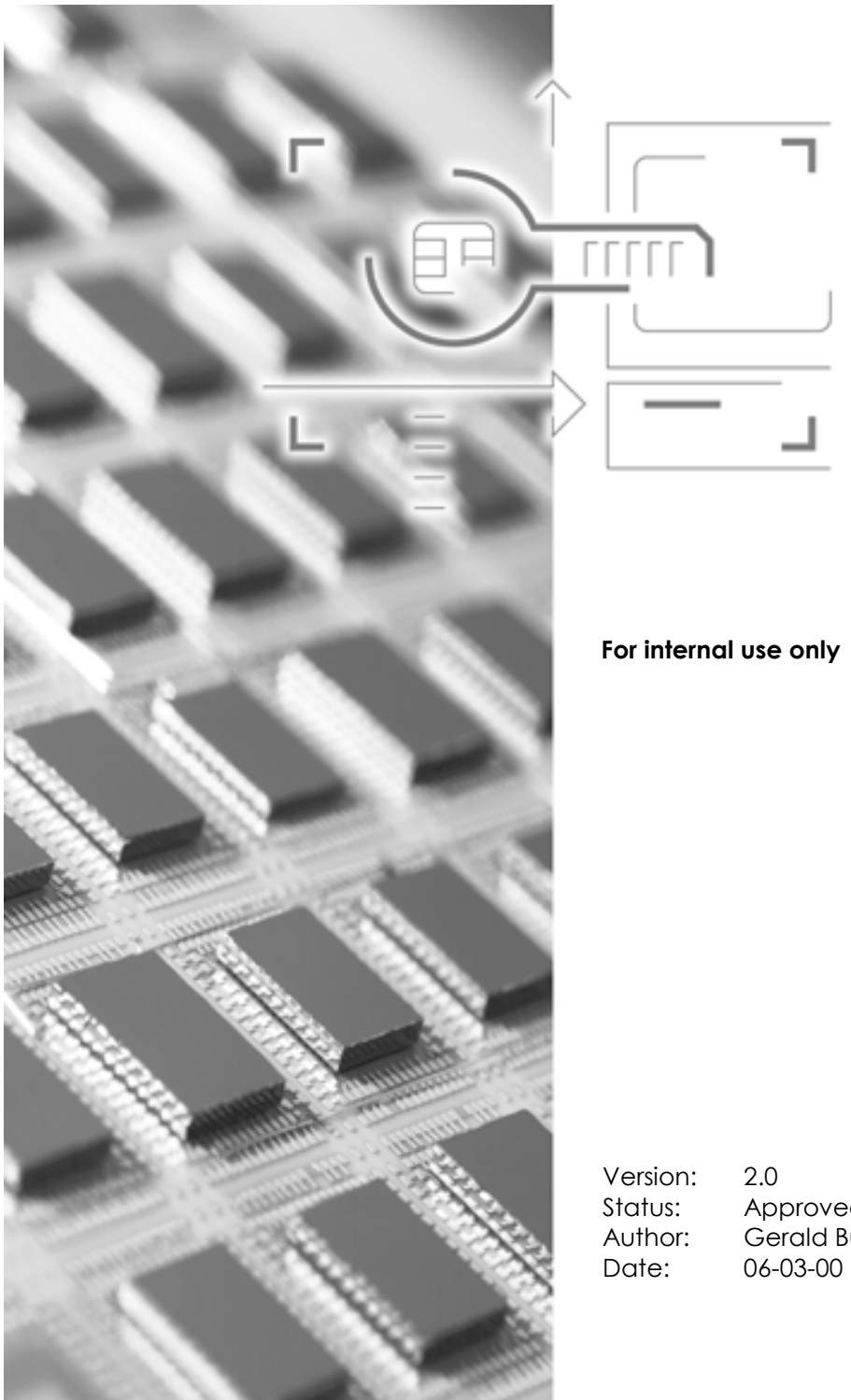
ab

IT Security Framework

IT Security Functional Policies

IT Security P&CC



For internal use only

Version: 2.0
Status: Approved
Author: Gerald Burri, IU43
Date: 06-03-00 17:42:00

Versioning

Version	Date	Status	Remarks
1.0	16.06.99	ITMM Approved	
2.0	06-03-00 17:42:00	Approved	By the IT Security Standards Committee

Co-author(s)

Name	Ref.	Contact	Function

Approval

Name	Ref.	Date	Visa
IT Security Standards Committee			

Distribution

Name	Ref.	Contact	Function

Changes

Basis Version	Changes

Referenced Documents

Ref.	Title
	Information Security Policy Statement

Further Information

File name	FunctionalPoliciesV20.doc
File format	Word 97
Location	READ

Table of Contents

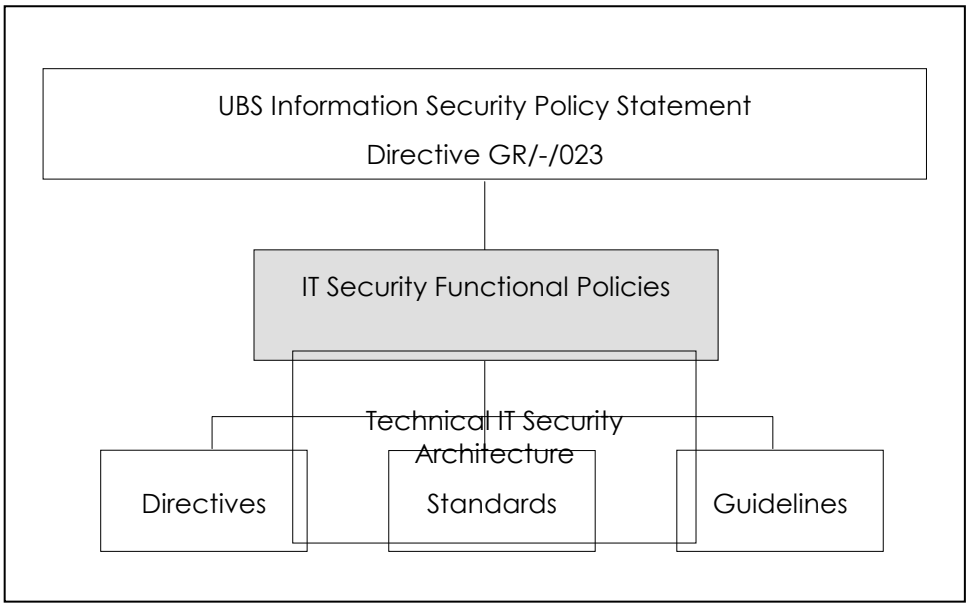
1 Introduction

1.1 Overview

The *Functional Policies* for UBS are derived from the *Information Security Policy Statement* of UBS. Its purpose is to provide general strategies for handling *IT security* within UBS.

The *functional policies* themselves serve as a basis to the Technical IT Security Architecture, *Directives*, *Standards* and *Guidelines*.

The relationship of these documents which make up the IT Security Documentation Framework is set out in the figure below:



1.2 Purpose and Scope of the IT Security Functional Policies

The *functional policies* apply to all IT users as well as to all *IT assets* and processes within the scope of UBS.

The scope of the *functional policies* begins with the electronic input of *data* and ends with its output on an electronic or non-electronic output medium. Additional security measures may apply to *IT assets* in paper form after leaving the printer.

1.3 Target Audience

The addressees of the *functional policies* are mainly IT managers, IT project managers, IT systems developers, IT security officers, IT security specialists and the BTCs, and where appropriate, end-users are addressed too.

1.4 Compliance / Applicability

Compliance with IT security *functional policies* is mandatory. If an IT user violates the provisions in an IT security policy or the derived d*irectives* and *standards*, either by negligence or intent, UBS reserves the right to take appropriate measures as defined by Human Resources up to and including termination.

All IT users are obliged to continue protecting UBS's *data* by observing IT security *functional policies* after the termination of employment with UBS.

External consultants, contractors, temporaries or third-parties must be subject to the same *IT security* requirements and have the same *IT security* responsibilities as UBS's employees.

1.5 Exceptions

Exceptions to any functional policy may be made, but must be approved by *IT Security* or, depending on the degree of risks, the appropriate IT Security Committee, which may require higher level management *authorization*. All exceptions to *functional policies* are formally recorded, tracked, and reviewed by *IT Security*.

1.6 Reading this document

In this document some terms are used either in the interest of brevity or as placeholder for other and/or more complex terms.

"UBS" currently stands for P&CC Division.

"IT" followed by a subject stands for "Information Technology" (e.g. *IT asset*). Without a subject "IT" stands for the IT department (e.g. … approved by IT.).

"*IT Security*" refers to the UBS IT Security Department.

"*IT security*" refers to the provision of organizational, technical and social measures necessary to safeguard *IT assets* against unauthorized access, against damage and interference - both malicious and accidental as well as against lost respectively recovery in case of damage or lost.

"IT user" is a general term for all kind of people using UBS' IT equipment, i.e. employees, contractors, consultants, providers, temporaries, or *third parties* in their role as end-user, developer, system administrator, computer operator etc. Where a particular group of IT users has to be addressed, it will be expressed by its propre denotation (e.g. end-user, developer etc.).

"IT" and/or or "IT security" may be omitted in the text; however, the reader should keep in mind that this entire policy set relates only to IT and IT security phenomena, e.g. *functional policies* instead of IT security *functional policies*.

For all terms printed in italic an explanation can be found in the glossary at end of the document.

2 Security Objectives and Principles

2.1 Objectives

The objectives of the *functional policies* are derived from the IT security fundamentals laid out in the *Information Security Policy Statement*. Partly amended, they read as follows:

IT asset ownership	IT asset owner accountability for determining, implementing, and maintaining adequate security for all *IT assets* must be included.
Confidentiality, *integrity*, *availability*, *non-repudiation*	The categorization or differentiation of classification levels according to asset security needs and the functions being performed must be included. *Confidentiality*, *availability*, *integrity*, and *non-repudiation* of any and all *data* that is generated, stored, processed or transferred by *IT assets* must always be guaranteed according to business needs, UBS classification *procedures*, and any legal or contractual constraints.
Storing, processing and transmitting *data*	Classification of *data* and the appropriate security measures apply to all *data* storage, process and transmission actions.
Separation of duties	A real and lasting separation of authority/responsibility between *IT security* service tasks and *IT security* control tasks must be forced. This separation must also exist between development tasks and production tasks as well as for access request, approval and granting tasks.
Access Control	No computer resources may be used without individual log-in. All *IT assets* must have IT security measures implemented such that access cannot be gained by unauthorized IT users. Read only access *IT assets* up to „Internal Use Only“ may be granted without specific *access control* (e.g. BankWeb)
"Need to know" "Need to do" (Least privilege)	Every IT user must only have access to the *data* and functionality necessary to do his or her job. Access to *IT assets* classified as "Confidential" or higher must be explicitly authorized, the default being no access.
Application development and change control	The thorough incorporation of appropriate security measures must be ensured. *IT security* must be a key consideration of all phases of application development, from concept to final implementation, including change control.

Appropriate IT security measures	The concept of a baseline security level of control measures on commonly used *IT assets* must be included. This has to be extended by enhanced levels when specifically required. *IT security* always has to meet the security needs of UBS and its clients. The measures being applied shall not exceed these needs, i.e. if an activity is to be viable for UBS, the efforts, rewards, and risks must all be in reasonable proportion.
Documentation	All security requirements and the measures implemented to meet them must always be fully documented and kept up-to-date over time.
Compliance monitoring	Audit functions must be included to detect breaches, anomalies, and unauthorized actions, as well as to check compliance with the IT security *functional policies*, *directives, standards* and *procedures*.
Incident handling	The detection and reporting of suspected and/or known security deficiencies and violations must be facilitated.
Maintenance of *trust*	*IT security* must always be maintained at the predefined level that will not compromise the sanctity of the *trusted environment*.
Fail-safe stance	If an *IT system* or an IT security measure fails, it must fail in such a way that access is denied, rather than granted in an uncontrolled way. This may result in denying access to legitimate IT users as well, until repairs are made.
Security awareness	All UBS IT users must always be kept aware of the risks faced by the business when using *IT assets*, and must be informed about the use of necessary security measures. They have to understand the need for their personal contribution.
Individual accountability	Every IT user must be obliged to be responsible for security actions as defined by his or her *role* or taken under his or her identity.
Benefit to UBS	*IT security* must support UBS in its endeavors to assure stability, quality, and long-term viability.
Benefit to individuals	*IT security* must support UBS IT users to properly fulfil their tasks and maintain their security awareness and responsibilities.

2.2 Principles

To fulfil the *functional policies*' objectives the following principles are guidance to appropriate *functional policies*, *directives*, *standards* and *guidelines*:

- *IT security* is everyone's duty and responsibility on a day-to-day basis. Specific responsibility for *IT security* is NOT solely vested in *IT Security*.
- *Functional policies*, *directives*, *guidelines* and *standards*, and day-to-day execution of IT security measures must always be consistent with the objectives.
- IT security decisions and issue dispositions are be based on robust risk analyses.
- Risk elimination shall be considered first before risk reduction. If neither of these are feasible, risk transferring to a *third party* or even risk avoidance has to be considered.

- Preventive IT security measures shall be considered first before detective ones and these prior to reparative ones.
- Technical IT security measures shall be considered first before organizational ones.
- International or industry standard approved security tools and methods must be considered prior to in-house built ones ("buy not make").
- IT security management evolves to general *standards* and methods with execution and accountability distributed by region and/or business entities when appropriate.
- *IT security* includes continuing reviews of the business value of the security measures already in place.
- UBS's IT security measures are always "just in time" and "time to market".
- IT security staff always acts proactive rather than reactive.
- *IT security* always meets the requirements of a changing environment. The correct rate of change is more important than the static environment at any given time.
- UBS IT security tools, methods and practices do not rely on their secrecy in order to be effective ("no security by obscurity").
- All computer and communications security measures must be simple and easy to use, simple and easy to administer, and simple and easy to audit.
- All IT security measures must be accepted and supported both by the people who are monitored by and those who work with the measures.
- UBS adheres to all legal and regulatory requirements.
- No UBS organization must compromise the security of any other UBS organization.
- Each *IT asset* is classified according to its requirements with respect to *confidentiality*, *integrity*, *availability* and *non-repudiation*.
- Reviews of IT security measures are not performed by persons responsible for implementing and maintaining security measures.
- The minimum requirement for protecting *IT assets* regardless of the classification is *access control*. i.e. IT user *authorization*, *authentication* and *privilege control*.

3 Security Organization

3.1 Roles and Responsibilities for IT security

3.1.1 Management

3.1.1.1 Due Diligence

All managers in UBS are responsible for implementing IT security measures in a manner that is consistent with generally accepted business practices.

3.1.1.2 Handling Variances

Managers are responsible for noting variances from generally accepted IT security control practices, and also for promptly initiating corrective actions.

3.1.1.3 IT security Compliance

UBS management must prepare periodical plans for bringing its computer and communications systems into compliance with published policies and *standards*.

3.1.1.4 Control of System Use

The responsibility for ensuring the correct use of UBS *IT systems* lies with line management.

3.1.1.5 Return of *Data* and *IT Assets*

When an individual's relationship with UBS terminates, it is the responsibility of the immediate manager to ensure that all *information* and IT equipment in the custody of the individual is returned to UBS.

3.1.1.6 Non-Reliance on a Single Person

At least two available persons must possess expertise in important computer or communications related areas.

3.1.1.7 Reporting of *IT security* Relevant Changes

Business management must report all changes of IT security responsibilities to *IT Security*.

3.1.1.8 Confidentiality Agreements

All IT users must sign or be party to a *confidentiality* agreement at the time they join UBS and before being granted access to any UBS *IT asset*.

3.1.1.9 Accordance to IT security Policies, *Directives Standards* and *Procedures*

Every IT user must understand UBS's policies, *directives*, *standards* and *procedures* about *IT security*, and must agree in writing to perform his or her work according to these.

3.1.1.10 Review of End-User Back-Up Process

Line managers must make sure that proper back-ups of *critical data* are being made if such *data* is resident in the end-user computing environment.

3.1.1.11 Independent Review of IT security Measures

An independent review of IT security measures must be periodically obtained. These reviews must include efforts to determine both the adequacy of and adherence to IT security measures. The reviews must not be performed by persons responsible for implementing and maintaining security measures.

3.1.1.12 *Separation of Duties* and Control Over UBS Assets

Whenever a UBS *IT system*-based process involves *sensitive or critical data*, the *IT system*

must include measures enforcing a *separation of duties* or other compensating control measures. These control measures must ensure that no one individual has exclusive control over this type of UBS *IT assets*.

3.1.1.13 IT security Management Committees

One or more IT security management committee must be composed of senior managers and/or IT security experts or their delegates from each of UBS's major divisions. The committee(s) meet(s) regularly to perform necessary high-level IT security management activities as well as to review the current status of UBS's IT security, approve and review IT security projects, and approve new or modified IT security policies, *directives* and *standards*.

3.1.1.14 IT Asset Ownership

All *IT assets* must have a designated owner. Management must assign ownership responsibility.

3.1.1.15 Delegation of IT Asset Owner Duties

An IT asset owner's responsibility for the specification of appropriate IT security measures must not be delegated to service providers outside UBS unless approved by *IT Security*.

3.1.1.16 Ownership of Business Assets

IT must not be the owner of any business *data*, applications and systems.

3.1.2 IT Security Organization

3.1.2.1 Responsibilities for *IT security*

Guidance, direction, and authority for all IT security activities is assigned to *IT Security*. The respective IT engineering and IT operations units are responsible for the secure development, implementation and operation.

3.1.2.2 *IT Security*'s Mission

IT Security is charged with the prevention of serious loss, damage or compromise of the entirety of UBS's *IT assets*. It must co-ordinate and direct specific actions that will help to provide a secure and stable IT systems environment consistent with UBS goals and objectives. The Department must provide the direction and technical expertise to ensure that UBS's *data* and other *IT assets* are properly protected.

3.1.2.3 Tasks of *IT Security*

IT Security is responsible for establishing and maintaining UBS-wide IT security policies, *directives*, *standards*, *guidelines* and *procedures*. The focus of these activities is on *data* electronically stored, processed or transmitted on UBS computer and communication systems, no matter what form it takes, no matter what technology is used to handle it, no matter where it resides and no matter who the owner is. The Department acts as a liaison on *IT security* matters between all UBS departments and divisions, and must be the focal point for all IT security activities throughout UBS.

3.1.2.4 *Risk Management* Responsibilities of *IT Security*

IT Security is responsible for:

- defining and documenting the processes involved in IT security *risk management*
- maintaining a register documenting how any known IT security risks are managed
- detect and assess new threats, and bring them to the attention of system owners or the respective custodians

3.1.3 IT Product and Service Providers

3.1.3.1 Project Managers

Managers of IT projects must ensure that IT security considerations are properly included

in the entire life cycle of the projects, from planning all the way through rollout and maintenance. The applications and infrastructure systems must meet all security requirements defined by *IT assets* owners, and the IT security policies, *directives* and *standards*.

3.1.3.2 Systems Developers

Systems Developers are responsible for the secure development and implementation of application and infrastructure systems according to the requirements defined by the project management, and the IT security policies, *directives* and *standards*.

3.1.3.3 IT Operations

IT operations managers are responsible for the secure installation and operation of *IT systems*. These systems must comply with all security measures defined by the owners of the *IT assets* (data and application owners), and the IT security policies, *directives* and *standards*.

3.1.3.4 Reporting of *IT security* Relevant Changes

Service providers must report all *IT security* relevant environmental changes to *IT Security* promptly. Such changes include e.g. changes of physical access means, changes of IT security responsibilities, and changes of established IT security measures.

3.1.4 IT Asset Owners

3.1.4.1 Accountability / Responsibility of all IT Asset Owners

IT asset owners are responsible for making and communicating judgements and decisions on behalf of UBS with regard to the use, classification, and protection of a specific *IT asset*. They are accountable for classifying *IT assets* according to the required degree of *confidentiality*, *integrity*, *availability* and *non-repudiation* and defining the specific set of security measures to be applied by the IT users during handling the *IT asset*.

3.1.4.2 Specific Responsibilities of Data Owners

Data Owners must decide about who (users, processes, applications, systems etc.) will be permitted to access the *data*, and the uses to which this *data* will be put.

3.1.4.3 Specific Responsibilities of Application Owners

Application owners are responsible for designing, developing, and implementing applications such that the applications maintain the proper classification of *confidentiality*, *integrity*, and *availability* of the input *data* and all derivative *data*.

3.1.4.4 Specific Responsibilities of System Owners

System owners are responsible for secure operation and administration of *IT systems*, and defining, implementing and maintaining IT security measures, both technical and organizational, consistent with the instructions of the data and application owners.

3.1.4.5 *Risk Management* Responsibilities of IT Asset Owners

All owners of *IT systems* are responsible for:

- having the security risks assessed prior to starting the operation of a particular *IT asset*
- having the security risks re-assessed periodically or upon appearance of new threats, throughout the lifetime of an *IT asset*
- accepting the residual risks involved in operating such *IT asset*, according to the UBS Information Security Risk Policy

3.1.5 IT Asset Custodian

3.1.5.1 Specific Responsibilities of Custodians

Custodians are entrusted with certain IT asset owner responsibilities, particularly for

- defining specific control *procedures*
- implementing and maintaining IT security measures
- administering IT security measures and
- providing recovery capabilities

consistent with the instructions of the IT asset owners.

3.1.6 IT Users

3.1.6.1 Accountability of IT Users

IT users are accountable for protecting and treating UBS's *IT assets* consistent with the assets' classification levels, and for complying with the IT security measures requirements specified by the IT asset owners and/or custodians.

3.1.6.2 Use of UBS *IT Systems*

UBS computer and communications systems must primarily be used for authorized business purposes. The limited use for private purposes is permissible under the condition that the use is not abusive, is not for commercial purposes and the system load as well as the system security will not be jeopardized.

3.1.6.3 Leaving Sensitive Systems

If the *IT system* to which they are connected contains *sensitive or critical data*, IT users must not leave their workstation unattended without first blanking the screen, suspending the session or logging-out.

3.1.6.4 Back-up of Locally Held *Data*

Whenever *data* is held locally, IT users are responsible for ensuring that such *data* is properly backed up and recoverable.

3.1.6.5 *Risk Management* Responsibilities of End-Users

Anybody accessing a UBS *IT system* is responsible for reporting all observed or suspected IT *security incidents* or vulnerabilities as quickly as possible according the *IT Security* approved *procedures*.

3.1.6.6 Unauthorized Access

IT users are prohibited from gaining unauthorized access to any *IT asset* or from obtaining access control *mechanism* which could permit unauthorized access.

3.1.6.7 No Investigation of a Suspected Vulnerability

IT users must not test or attempt to compromise IT security measures nor to prove a suspected vulnerability unless specifically approved in advance and in writing by *IT Security*.

3.1.6.8 No Exploiting of IT security Vulnerabilities

IT users must not exploit vulnerabilities or deficiencies in *IT security*.

3.1.6.9 No Disclosure of IT security Measures Specifics

No *information* of the nature listed below must be disclosed to persons who do not have a valid "Need-to-Know":

- IT security measures that are in use, or the way in which they are implemented
- Programming source code, executables or binaries of IT security measures.

3.1.6.10 No Disclosure of IT security Vulnerabilities

No *information* of the nature listed below must be disclosed to persons who do not have a valid "Need-to-Know":

- Specific *information* about *IT security* vulnerabilities, such as the specifics of an IT system break-in
- Individuals, organizations, or specific *IT systems* that have been damaged by computer crimes and computer abuses

- Specific methods used or appropriate to exploit *IT security* vulnerabilities.

3.1.6.11 Unique Passwords for Each System

To prevent the compromise of multiple systems, IT users must employ a unique password for each system or application they have access to.

3.1.6.12 No Writing Down of Passwords

Passwords must not be written down and left in a place where persons might discover them.

3.1.6.13 No Password Sharing

Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized IT user.

3.1.6.14 Individual Accountability

IT users are responsible for all activities performed under their personal user accounts. They must not allow others to perform any activity with their *user-ID*.
User accounts must not be utilized by anyone other than the individuals to whom they have been issued, i.e. IT users are forbidden from performing any activity with *user-ID*s belonging to other IT users.

3.1.6.15 Passwords Protection

Passwords (also PINs or *keys* used for *authentication*) have to be treated as if classified as "Strictly Confidential." Passwords or *keys* for access to *data* classified as "Secret" have to be treated as if classified as "Secret".

3.1.6.16 Password Construction

All passwords must be of predefined length and structure in order to prevent successful trivial attacks in whatever form.

3.1.6.17 User-Chosen Passwords

IT users must not construct passwords which are identical or substantially similar to passwords that they had previously employed.

3.1.7 Other Organizations

3.1.7.1 Corporate Legal & Compliance

The Corporate Legal & Compliance Department is responsible for establishing rules to ensure compliance with all relevant laws pertaining to *IT security*.

3.1.7.2 Corporate Audit

The Corporate Audit Department is responsible for periodical reviews of the adequacy of and adherence to IT security measures.

3.1.7.3 Corporate Security

The Corporate Security Department has control over the physical aspect of *IT assets*. Corporate Security oversees access to restricted areas such as the computer rooms. Where a breach of *physical security* leads to an *IT security* violation, Corporate Security will investigate the *incident* in conjunction with *IT Security*.

4 IT security Risk Analysis and Management

4.1 IT security Risk Analysis and Management

4.1.1 IT security Risk Assessment for Assets

An IT security Risk Assessment as defined by *IT Security* is required for:

- any new or significantly modified *IT system*
- any placement of sensitive *information* into an *IT system*
- any extraction of sensitive *information* out of an *IT system*
- any outsourcing of an IT service
- any external IT connection the UBS network and an un*trusted* source or target

4.1.2 IT security Risk Assessment Time

Any *IT asset* placed into production use within UBS must be subject to a risk assessment on the occasions listed below:

- initially, prior to being placed into production use
- periodically during production use
- upon appearance of new threats

4.2 Selection of IT security measures

4.2.1 Hardware and Software Procurement

To assure compliance with in-house IT security *standards*, all hardware and software must be procured through standard purchasing channels.

4.2.2 Independent Security Systems

With the exception of *trusted systems* or within *trusted domains* or *trusted* chains, the security of an *IT system* must never be entirely dependent on the security of other *IT systems*.

4.3 Handling of IT security Problems

4.3.1 *Incident* Reporting *Procedure*

A formal *procedure* for reporting observed or suspected IT *security incidents* or deficiencies must be established by *IT Security*.

4.3.2 *Incident* Response *Procedure*

A formal *incident* response *procedure* must be established, defining clearly:

- the individuals responsible for handling IT *security incidents*
- the actions to be taken upon receipt of an *incident* report

4.3.3 Involvement of *IT Security*

All *IT security* problems must be handled with the involvement and cooperation of *IT Security* staff. The use of external consultants, computer security response teams, or other outsiders is specifically prohibited unless these have been approved by *IT Security*.

5 Information Sensitivity and Risks

5.1 Data Classification and Handling

5.1.1 Classification by the Owner

Each data asset must be classified according to its requirements with respect to *confidentiality*, *integrity*, *availability* and *non-repudiation*. Responsibility for setting or changing the classification of an data asset lies with the data owner.

5.1.2 Use of *Data*

UBS *data* must be used exclusively for authorized business purposes.

5.1.3 Duplication of *Data*

"Need-to-Know" and "Least Privilege" principles must be adhered to in replicating, disseminating and deleting *data* and data sets.

5.1.4 Storage, Processing and Transmission *Data*

The classification and the defined security measures and instructions of the original data asset must apply to all *data* storage, processing and transmission actions.

5.1.5 Down-Loading *Sensitive Data*

Sensitive UBS *data* must be down-loaded from a mainframe or server to an IT user's personal computer environment only after three conditions are fulfilled:

- a clear business need must exist
- advance permission from the data owner or custodian has been obtained
- downloads must be logged

5.1.6 Custodian *Role*

When *data* is transferred, for example to an IT user's personal computer environment, the recipient must assume responsibility for that *data*, its protection and further use according to its original classification and instructions.

5.2 Data Privacy

5.2.1 Privacy of Personal Files and Messages

UBS makes all efforts to respect the privacy of its staff's personal files and personal mails stored, processed or transmitted on UBS *IT systems*. This means that all other IT-users, including managers and system administrators or operators, must not read, nor have access to, such personal files.

Exceptions may be made if the action is part of:

- a formal investigation initiated by Human Resources, Corporate Legal & Compliance or Corporate Security in conjunction with *IT Security*
- a recovery action from an operational problem or *IT security* breach
- an effort to dispose of or reassign files after a IT-user has left UBS.

However, the task of system administration and operation may occasionally lead to the unavoidable possibility of support personnel having access to such *data*. In such a case UBS must make sure that the support personnel respects the privacy of the *data*.

5.2.2 Observation of User System Usage

UBS does not routinely engage in the observation of IT system usage at the individual's level or in monitoring of IT user behavior.

Exceptions may be made, if the action is:

- part of a formal investigation initiated by Human Resources, Corporate Legal & Compliance or Corporate Security in conjunction with *IT Security*
- necessary in order to guarantee the security or operability of UBS's *IT systems*

Exceptions as to 2nd bullet are subject to the policies section "*Logging* and Monitoring", as well.

5.2.3 Formal Monitoring *Procedure*

A formal monitoring *procedure* must be established, defining clearly:

- how to apply for the monitoring of an IT user's system usage
- the individuals entitled to arrange for such monitoring
- the individuals entitled to have knowledge of the results of such monitoring
- the actions to be taken prior, during, and after such monitoring action

5.3 Data Confidentiality

5.3.1 Classification Scheme for *Data Confidentiality*

In line with UBS *directive* CR/-/001,the classifications for *data confidentiality* are "Public", "Internal Use Only", "Confidential", "Strictly Confidential", and "Secret".

Any data asset that is not explicitly classified has a default classification of "Internal Use Only".

5.3.2 Multiple *Data Classifications* On Single *IT System*

If an *IT system* contains *data* with varying sensitivity classifications, the security measures used must reflect the most *sensitive data* on the *IT system*.

5.3.3 Storage *Media* Upgrade

If *data* recorded on computer storage *media* with a higher sensitivity classification is moved to *media* with a lower sensitivity classification, then the *media* with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity classification.

5.3.4 Storage and Transmission of *Non-public Data*

Data classified as "Internal Use Only" or "Confidential" must be encrypted when stored on transportable *media* without physical access protection, or when transmitted over public networks.
Data classified as "Confidential" or higher must be encrypted on internal networks, as well, even when they are resident in UBS premises.

5.3.5 Storage and Transmission of "Strictly Confidential" *Data*

Data classified as "Strictly Confidential" *data* must always be encrypted when being stored or transmitted, regardless of the location, storage medium, or the way in which it is transmitted.
Data classified as "Strictly Confidential" or higher must be stored only on *IT systems* whose operational responsibilities are in the hands of UBS (no outsourcing).

5.3.6 Storage, Processing and Transmission of "Secret" *Data*

Data classified as "Secret" must be stored, processed or transmitted on *IT systems* only if the *IT systems* are classified for processing such *data* and the following ruled are applied:

- the *IT systems* is not connected to any network or any computer
- the *IT systems* are switched off if not use a significant period of time
- the *IT systems* are provided with a power down process to clear any caches and remove all temporary files
- the *IT systems* are located in an area with strict physical access control
- the *IT systems* are placed in locations providing adequate protection against

"TEMPEST" attacks

5.3.7 Recycling, Deletion and Destruction of *Sensitive Data*

When no longer used, all *data* classified as "confidential" or higher must be properly deleted from the *media*, with no residue remaining which could be recovered.

5.3.8 Labeling of IT System Output

Output from *IT systems* containing classified *data* must carry an appropriate classification label. The marking must reflect the classification of the most *sensitive data* in the output.

5.4 Data Integrity

5.4.1 Measures for *Data Integrity*

Measures to guarantee *data integrity* are chosen based on impact analyses.

5.5 Data Availability

Further policy statements on *availability* can be found in "11, Disaster Recovery/Business Continuity".

5.5.1 Measures for *Data Availability*

Measures to guarantee *data availability* are chosen based on impact analyses according to the costs of reconstruction.

5.6 Data Non-Repudiation

5.6.1 Classification Scheme for *Non-Repudiation*

The classifications for *data non-repudiation* are "Non-repudiation not required" and "Non-repudiation required".

Any *data* asset that is not explicitly classified has a default classification of "Non-repudiation not required"

5.6.2 Storage, Processing and Transmission of *Data* Classified as "Non-repudiation required"

Data non-repudiation shall be ensured by the use of electronic and logical measures, such as *digital signatures* which provide unforgeable proof of shipment and/or receipt of *data*.

5.7 Intellectual Property Rights

5.7.1 Installation of Copyrighted *Data* and Software

Copyrighted *data* and software, that UBS does not have specific approval to store and/or use, must not be stored on UBS *IT systems* or networks.

5.7.2 Supply of Software Needed for Business Activities

UBS management must provide a sufficient number of licensed copies of software such that IT-users can get their work done in an expedient and effective manner.

5.7.3 Handling of *Third Party* Confidential and Proprietary *Data*

Unless specified otherwise by contract, all confidential or proprietary *data* that has been entrusted to UBS by a *third party* must be protected as though it was UBS confidential *data*.

5.7.4 Making Additional Copies of Software

Third party software in the possession of UBS must not be copied to any storage *media*, transferred to another computer, or disclosed to outside parties, unless such copying is consistent with relevant license agreements, and either:

- management has previously approved of such copying, or
- copies are being made for contingency planning purposes.

5.7.5 Rights to Intellectual Property

Intellectual property developed or conceived of while an employee, contractor, consultant etc. is working for UBS is the exclusive property of UBS, unless special arrangement have been made.

5.7.6 Legal Ownership of *IT Systems* Files and Messages

UBS has legal ownership of the contents of all files stored on its computer and network systems as well as all messages transmitted via these systems. UBS reserves the right to access this *data* without prior notice whenever there is a genuine business need. Exception: This policy does not apply to all *information* subject to section "Data Privacy" above.

6 Hardware and Software Security

6.1 Access Control

6.1.1 Authorization

6.1.1.1 Privilege Authority

Basic rights and privileges are determined by the organization to which the individual is assigned, as specified by Human Resources. Modifications to an individual's basic rights and privileges must be done only on the authority of the individual's manager.

6.1.1.2 Default Access Permissions

For each operational function (business *role*), there must be a set of access rights in the form of a default profile.

6.1.1.3 Group Access Rights (Business *Roles*)

Access to specific applications or *data* may be authorized for nominated groups of people through the specific configuration of a group profile. Membership of this group leaves the access rights to the individual IT user.

6.1.1.4 Fail Safe Stance Principle

If a computer or network access control system is not functioning properly, it must default to minimal privileges for authorized IT-users.

6.1.1.5 Individualized System Access

Computer and communication system *access control* must be achieved via *user-ID* and password which are unique to each individual IT user. *Access control* to files, databases, computers, and other system resources via shared accounts and passwords (also called lockwords) is prohibited.

6.1.1.6 Minimum *Authorization* Process

Any individual must be given the opportunity to apply for all business *roles* and access profiles and rights in every UBS system.
Any application for access must be authorized by

a) the superior of the applying individual
   and
b) the owner or custodian of the *IT asset* to be accessed
   and, optionally,
c) any additional *authorization* authority

6.1.1.7 Removal of Access Rights and Privileges

The access rights and privileges of staff who change their business function or organizational unit, or leave the employment of UBS, must be removed immediately upon their departure. All *user-ID*s must have the associated privileges revoked if no longer needed.

6.1.1.8 *Authorization* of Access Rights and Privileges

Access to UBS *data* and IT applications classified as "Confidential" or higher must always be authorized in advance by the data owner and the application owner respectively The application and the modification records must be kept as long as required by the needs of UBS.

6.1.1.9 *Separation of Functions*

The *authorization* systems and *procedures* must support a clear *separation of functions* such as request, approval and entry of access rights.

6.1.1.10 Use Of Standard *Authorization* Processes

For all IT applications and IT systems access request, approval and granting, the established standard *authorization procedures* and infrastructure must be applied.

6.1.1.11 Review of User Rights and Privileges

Rights and privileges granted to IT users must periodically be re-certified by their management and the asset owners.

6.1.1.12 Disabled User Accounts

User accounts must be disabled when no longer needed, or when they have been inactive for a certain period of time.

6.1.1.13 Re-use of *User-ID*'s

User-Ids must not be re-used until all accounts belonging to this ID have been deleted.

6.1.1.14 Cross-Location *Access Control*

Where there are cross-border access and transfer restrictions on *sensitive data* assets, those assets must be restricted. The mode used must be based on business value, the relevant legal restrictions, and consideration of local practices and customs.

6.1.2 Identification

6.1.2.1 *User-ID* Uniqueness

Each *user-ID* or account on a UBS system must uniquely identify only one IT user or *IT process*.

6.1.2.2 Shared Accounts

Shared accounts or shared logins for groups must be avoided. When there is no sensible alternative, a group account may be used but must have clear responsibility assigned to one individual.

6.1.2.3 Different *Authentication Credentials* for Systems Administrators

IT systems administrators must execute their duties as administrator and their day-to-day work of an ordinary user under different *authentication Credentials*.

6.1.3 Authentication

Description of "*Strong Authentication*" see chapter "6.2, *Encryption* & *Authentication*".

6.1.3.1 Levels of *Authentication*

UBS aims *strong authentication* everywhere and every time. Until all legacy applications/legacy infrastructure are replaced, the following policy must be applied: *Strong authentication mechanisms* must be employed when accessing, storing, processing or transmitting *data* classified as "Confidential" or above. *Simple authentication mechanisms* are sufficient when accessing, storing, processing or transmitting *data* classified below "Confidential".

6.1.3.2 Use Of Standard *Authentication* Processes

In all IT applications and systems, the established standard *authentication mechanisms* must be applied.

6.1.3.3 Single Sign-On Process

A single request for *user authentication* must be given at the time the IT user accesses UBS's IT systems environment. For this purpose, a general single sign-on *mechanism* has

to be provided and employed.

6.1.4 Credentials and Keys used for Authentication

"*Key Management*" see chapter "6.2, *Encryption* & *Authentication*".

6.1.4.1 Display and Printing of Passwords

The display and printing of passwords must be obscured so that unauthorized parties will not be able to observe or subsequently recover them.

6.1.4.2 Periodic Forced Password Changes

All IT users must be automatically forced to change their passwords after a reasonable period of time depending of the sensitivity of the asset.

6.1.4.3 Assignment of New or Expired Passwords

The initial passwords must be valid only for the involved IT user's first on-line session. At that time, the IT user must be forced to choose a different password before any other work can be done.

6.1.4.4 Unsuccessful Password Entries

The number of consecutive attempts to enter an incorrect password must be limited. The *user-ID* must be suspended until reset by a system administrator after a predetermined number of unsuccessful attempts have been made to enter a password.

6.1.4.5 Processing Passwords

Fixed passwords must never be in readable form outside a workstation.

6.1.4.6 Storage of Passwords

Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without *access control*, or in other locations where they may be compromised.

6.1.4.7 Incorporation of Passwords into Software

Passwords must never be hard-coded (incorporated) into UBS in-house developed or modified software.

6.1.4.8 *Encryption* of Passwords

Passwords must always be encrypted when held in storage for a significant period of time or when transmitted over networks.

6.1.5 User Interface

6.1.5.1 Disclosure of Incorrect Log-In *Information*

When logging into a UBS computer or communications system, if any part of the log-in sequence is incorrect, the IT user must not be given specific feedback indicating the source of the problem. Instead, the IT user must simply be informed that the log-in process was incorrect.

6.1.5.2 Login Warning Banner

Prior to IT *user authentication*, the system must display a login warning banner. All login warning banners must meet all legal requirements of the country where the computer is used. The banners must not disclose any organizational *information* and must precede the system login process.

6.1.5.3 Login Screen

Login screens must simply ask the IT user to login, providing prompts as necessary. No further *information* must be provided until the IT user has successfully logged in.

6.1.5.4 Notice of Last Login

After login, the IT user must be given *information* reflecting the last login time, date as well as the number of and time of any unsuccessful login attempts.

6.1.5.5 Automatic Lock Screen

When a user session remains unused for a predefined period of time or is left unattended, the system must invoke a *screen saver* or session suspension *mechanism*. Re-establishment of the session must only occur after the IT user has been properly authenticated.

6.1.6 Privilege Control

6.1.6.1 Software Access Control *Mechanisms*

All application and infrastructure software installed on UBS *IT systems* must employ established standard access control *mechanisms*.

6.2 Encryption & Authentication

6.2.1 Approval for *Encryption* and *Authentication* Processes

Encryption and *authentication* processes (algorithms) applied to UBS *data* must be accepted in advance according an *IT Security* approved standard.

6.2.2 Assignment of *Key Management* Functions

Whenever *encryption* or *authentication* is used to protect *sensitive data*, the relevant owner(s) of the *data* must explicitly assign responsibility for *key management*.

6.2.3 Separate *Keys* for *Encryption* and *Authentication*

If both *encryption* and *authentication* are used, separate *keys* shall be used for each of these two control measures.

6.2.4 Control over *Key Management* Systems

Only specifically authorized personnel are permitted to control and finally implement key-management and similarly sensitive *encryption* systems. External contractors must sign a specific agreement.

6.2.5 Special Approval for Disclosure of *Encryption Keys*

Encryption keys must be classified as 'Strictly Confidential'. *Encryption keys* must not be revealed to consultants, contractors or other *third parties* unless the approval of a senior management is obtained.

6.2.6 Handling of *Certificate Authority Keys* and *Encryption Master Keys*

UBS systems must be designed so that no single person has full knowledge of *Certificate Authority keys* or *encryption master keys*. This must be achieved by *separation of duties* or *dual control* or by other appropriate means (e.g. by storing the *keys* in *tamper*-proof modules).

6.2.7 Life Time of *Encryption* and *Authentication Keys*

Whenever *encryption* or *authentication* is used to protect UBS *data*, the *keys* must be changed at reasonable intervals to protect *confidentiality* and authenticity.

6.2.8 Generating *Encryption* and *Authentication Keys*

Whenever *encryption* or *authentication* is used, the corresponding *keys* must be generated using *IT Security* approved *mechanisms* .

6.2.9 Transmitting *Encryption* or *Authentication Keys*

If *encryption* or *authentication keys* have to be transmitted, either a separate channel (e.g. phone, paper) must be used, or the *keys* must be sent in encrypted form. The

encryption of *keys* shall be performed with an algorithm at least as strong as the underlying *data protection* algorithm.

6.2.10 Storing *Encryption* or *Authentication Keys*

Encryption or *authentication keys* must only be kept in memory or on non-*tamper* proof storage *media* if absolutely necessary and no longer than required. On non-*tamper* proof storage *media* they must always be kept in encrypted or irreversible form. Whenever possible *keys* shall not be revealed to un*trusted environments* (e.g. workstations). Instead, tamper proof modules (e.g. *smartcards*) shall be employed making not the *keys* but only *key*-related operations available.

6.2.11 Key Recovery of *Encryption Keys*

Keys used for *encryption* may be included in an internal carefully controlled *key* recovery arrangement. Such arrangements always require explicit approval by *IT Security*. The *keys* must not be made available to *third parties*.

6.2.12 Key Recovery of *Authentication Keys*

Keys exclusively used for *digital signatures* or *user authentication* must never be subject to *key* recovery. Note that Certification Authority *keys* are governed by a separate policy.

6.3 System Environment

6.3.1 Compliance with *IT security* Requirements

All software purchase, development and maintenance activities must comply with UBS *IT security* requirements. All software used within UBS must comply with all binding *IT security* regulations such as policies, *directives*, *standards* etc. This applies to in-house developed software as well as to *third party* software. It is the responsibility of the installing organization to verify this compliance before the products are is installed on UBS *IT systems*.

6.3.2 Vendor-Provided Written Integrity Statements

If procurement of *third party* software is being considered, management must obtain a written *integrity* statement from the involved vendor. This statement must provide assurances that the software in question does not contain undocumented features, does not contain hidden *mechanisms* that could be used to compromise the software's security, and will not require the modification or abandonment of security measures found in the operating system under which it runs.

6.3.3 Use of Approved Hardware and Software

Only IT approved computers, peripherals, and/or software must be attached to or installed on UBS systems or communication networks. Personal equipment, peripherals, and/or software must not be brought into UBS facilities without prior approval by IT.

6.3.4 Disabling Unnecessary Software Features

Features which are clearly unnecessary in the UBS computing environment must be disabled at the time when software on UBS production systems is installed.

6.3.5 Automatic Detection of End-User Application Programs

All *IT systems* must use approved *mechanisms* to detect unauthorized copies of third-party software and new and/or modified application programs developed by end-users.

6.3.6 Determining Status of System

Every production system must include a predefined set of tools to assist the security administrator in verifying the security status.

6.3.7 Software Updates

IT security related updates of *IT systems* must be employed immediately upon *availability*.

6.4 Malicious Code

6.4.1 Use of Virus Protection Software

The protection or at least the early detection of virus infections of *data* stored and in transit must be assured by the implementation of *IT Security* approved and up-to-date anti-virus and *integrity*-checking software on all concerned *IT systems*.

6.4.2 Individual Responsibility for *Media* Virus Checking

Individuals receiving data *media*, from within or outside UBS from any source, have the responsibility for ensuring it is checked for viruses before use. Similarly, individuals intending to pass on data *media* within UBS or to external *third parties* must ensure that it is first checked for viruses.

6.5 Prohibited Software

6.5.1 Inappropriate Content

Illegal and/or offending images and/or text involving racial, nudity or sexual themes must never be displayed, stored, processed or transmitted on UBS *IT systems*.

6.5.2 Exploiters

Programs that are designed to investigate and/or exploit UBS's IT security environment (including password crackers, scanners and other "hacking" tools) are prohibited, except when expressly authorized by *IT Security*.

6.5.3 Diagnostic Hardware and Software

The use of network and network packet diagnostic hardware and software, and programs of similar function, must only be used by designated systems and network administrators in conjunction with business tasks.

6.6 IT Systems Development

6.6.1 *IT security* in the IT Systems Development Lifecycle

An *IT Security* approved sign-off process has to be established to confirm that *IT security* is considered at all stages of the IT system development lifecycle, and to check that it satisfies all necessary IT security requirements prior to be used in the UBS production environment.

6.6.2 IT security Services in Systems Development

The technical and organizational binding of IT security services into applications must be based on standard interfaces and processes.

6.6.3 Systems Development Documentation

At all stages of the development life cycle, development staff must document both, technical and organizational aspects of how *IT security* has been considered and implemented. When first published, and after major revisions, such documentation must be issued to and accepted by an *IT Security* approved sign-off process.

6.6.4 Release of Live Production *Data* for Testing

The use of production *data* for development testing is prohibited. In these cases where production *data* is needed for testing, the *data* must be desensitized and approved by the data owner prior to release. Use of desensitized production *data* must never

jeopardize banking security or business-related privacy.

6.6.5 Training and Operations Documentation

Business application systems must not go into production until all business users and IT operations staff have received appropriate documentation and training how *security incidents* are to be handled.

6.6.6 Removal of All Special Access Paths

Prior to moving software to production status, all special access paths must be removed so that access can only be obtained via normal secured channels.

6.6.7 Functionality of *IT Systems* Developed In-House

Only those functions described in the approved system design document must be included in a production computer or communications system that has been developed in-house.

6.6.8 No Trap Doors To Circumvent Access Control

IT systems must not contain trap doors that circumvent the authorized access control *mechanisms*.

6.7 Security Logging and Monitoring

6.7.1 Log Content and Practice

6.7.1.1 Resources for *Logging* And Monitoring

All *IT systems* must be designed to provide sufficient resources in terms of e.g. computing power, storage space, or network bandwidth, to fulfil all *logging* and monitoring requirements.

6.7.1.2 Granting of Audibility

The *logging* and monitoring *information* provided by *IT systems* must ensure the audibility of security relevant events by both UBS internal auditors and well as external auditors.

Procedures must be in place which determine both definition and verification of audibility criteria.

6.7.1.3 Clock Synchronization

All computers which produce logs and/or audit trails must be time synchronized.

6.7.1.4 Logs on Application Systems

All production application systems which handle sensitive or critical UBS *data* must generate logs that show every addition, modification, and deletion to such *data*. These logs must support recovery of all system activities.

6.7.1.5 *Logging* System Changes

Changes to the system environment made by privileged access must be logged, particularly where those resources are not normally changed during standard operation. All commands issued by IT system operators or administrators must be traceable to specific individuals.

6.7.1.6 *Logging* of External Communications

Records must be kept of all network-based communication with external parties (such as Bank partners, customers, agencies and other *third parties*) for later analysis and/or reconstruction. This includes transmissions such as email, *data* feeds and Web-based access etc..

6.7.1.7 *Logging* and Reporting on Privileged *User-ID* Activity

All *user-ID* creation, deletion, and privilege change activity performed by security administrators and others with privileged *user-ID*s must be securely logged and reflected in periodic management reports. Furthermore all commands issued on *authorization* systems by security administrators must be traceable to specific individuals via the use of comprehensive logs and unique *user-ID*s.

6.7.1.8 Generation of Logs of Control Override Facilities Use (Firecalls)

In all instances where control override facilities are activated and/or IT security measures have been overridden, a firecall log must be generated showing both the changes made and the privileged commands that were used as well as the individuals involved.

6.7.2 Log Management

6.7.2.1 Storage, Protection and Secure Retention of Logs

All System logs must be securely transmitted and collected, protected and appropriately archived. All *logging data* must be maintained in a form that can neither be viewed by unauthorized persons nor be modified nor be deleted nor be deactivated. The interruption or corruption of log *data* must be recorded in independent logs.

6.7.2.2 Periodic Review of Security Logs

Records reflecting security relevant events must be periodically reviewed.

6.7.2.3 Review of Logs of Control Override Facilities Use (Firecalls)

Procedures must be in place to ensure that firecall logs are reviewed and that the use of override facilities was warranted, and these facilities were used in a correct manner.

6.7.2.4 Audit-Trails in Production Environments

Any Audit-Trails must be brought to the attention of IT Operations, and the requirements with respect to backup, storage and recovery must be defined by the owner of an Audit-Trail.

IT Operations is responsible for the appropriate storage and protection of Audit-Trails.

6.7.3 Monitoring

6.7.3.1 Monitoring of Network Traffic

Network traffic, both internal and cross-border, must be monitored for unusual activity.

6.7.3.2 Monitoring of External Access

IT systems to which external parties have access (such as client systems, Web servers, and dial-up support facilities) must have all transactions and system configuration changes monitored in real time, with alerts escalated to 24x7 personnel.

6.8 Secure Operations

6.8.1 Secure Physical Placement

All Production Systems, as well as Production Testing Systems containing client *data*, must be placed in security zones.

A security zone must have the following characteristics:

- Responsibility for the security zone must be assigned to one individual
- Access to the security zone must be restricted to a minimum
- Within a security zone, all *IT systems* must be connected to a proper production center LAN

6.8.2 Trusted Systems

IT Operations shall enforce the accreditation of operational systems as "trusted system" according to the applicable criteria for trusted system accreditation. IT Operations must not take responsibility for the security for not accredited systems and applications.

6.8.3 Change Control *Procedure* for Production Systems

All computer and communications applications and systems used for production processing at UBS must employ a formal written change control *procedure*, regardless whether built-in-house or vendor supplied.

6.8.4 Review of Production System Changes

Periodic reviews of production systems must be conducted to ensure that only authorized changes have been made.

6.8.5 Backup/Restore

IT Operations creates backup copies of all data assets on a regular basis, based on business requirements. It determines the frequency, operation time and storage locations based on the requirements for recovery in case of system or disk outage, or a disaster.

6.8.6 Privileged Access

All privileged access, be it for operational or other purposes, must be performed exclusively from within the same security zone which is under the control of the responsible IT Operations unit, or alternatively, from within a physically secured location using strong user-authentication and a secure channel.

6.8.7 Interventions for Support

Interventions for support which are not being performed by operations staff (i.e. 2nd level support), must be:

- requested by the responsible IT Operations unit
- limited to the necessary minimum both timewise and locationwise
- monitored by operations staff

6.8.8 Separation of Production Environment

Production systems must be protected from the effects of outages in other environments, such as office automation, development and production testing environment.

6.8.9 Compilers and Utilities on Production System

Compilers, assemblers or other general purpose utilities which may be used to perform development functions or otherwise compromise the security, must not be used on production computer systems.

6.8.10 Control Override Facilities (Firecalls)

Application and system development staff must not have access to production systems. This must only occur in emergency situations via the established standard Firecall *procedure*.

6.8.10.1 Establishment and Use of Control Override Facilities

Control override facilities (Firecalls) must only be used in exceptional circumstances where control *procedures* need to be changed for a limited time in order to maintain critical business operations.

6.8.10.2 Restoration of Normal Operations

All changes made during a Firecall situation must be fully restored to their original configuration. Permanent changes required must be made through the normal *procedures*.

6.8.11 Installation of Production Software and Hardware

IT Operations is exclusively responsible for installing new or modified production software and hardware components.

6.8.12 Outsourcing of operational responsibilities

- All UBS *functional policies*, *directives* and *standards* must be fulfilled
- A detailed outsourcing contract, approved by Legal and Compliance, with the external party has to define "rights and duties". All external operation staff have to sign a *confidentiality* agreement. The right to put *directives* in place must reside to UBS, especially IT Operations Security for operational matters
- UBS must have the right to monitor / check the system every time and without a pre-notice
- Physical access to the system for third-party operators must be possible only with the supervision from a UBS operator
- Data transfer out of the UBS network is forbidden. Exceptions have to be accepted by IT Operations Security.

6.8.13 Policy Compliance Checking

IT systems must be regularly checked for compliance with UBS security *standards*, as well as for security vulnerabilities publicized by vendors and computer emergency response alerts.

7 Communications and Network Security

7.1 Network Connections

7.1.1 Connection of *IT Systems* to UBS Network

Only UBS inventoried *IT systems* are allowed to be connected to the UBS network. This has to be done exclusively by authorized UBS personnel.

7.1.2 Avoiding Degradation of Network Security

Any connections between networks, sub-networks, network components, systems, or applications must be such that none of the participants suffer any degradation of security. Security must be maintained such that the sanctity of a *trusted* network is not compromised.

7.1.3 Connecting UBS Networks to *Third Party* Networks

All connections between public and UBS networks must be expressly authorized by *IT Security*.

7.1.4 Restricted Destinations

Third party connections over the internet must be restricted to DMZ (demilitarized zone) within *firewalls*. All other destinations, particularly to UBS production systems, must be explicitly excluded to *third parties*.

7.1.5 Direct Network Connections with *Third Party* Organizations

The establishment of a direct connection (e.g. *VPN tunnels*) between UBS systems and computers at external organizations, vendors or customers via the Internet or any other public network, is prohibited unless this connection has first been accepted by *IT Security* approved *procedures* (no "private" connections!).

7.1.6 Network-Connected Third-Party Systems

As a condition of gaining access to UBS's computer network, every *third party* must secure its own connected systems and network in a manner consistent with UBS requirements. UBS must immediately terminate network connections with all third-party systems not meeting the UBS requirements.

7.1.7 Internet Connections

All connections between UBS internal networks and the Internet (or any other publicly-accessible computer network) must include an approved *firewall* operated by network and security staff, and related *access control*.

7.1.8 External Network Connections

All in-bound dial-up lines or external connections to UBS internal networks and/or *IT systems* must pass through an additional access control point (e.g. *firewall*, gateway, or access server) before IT users can reach a login banner. Computers which use modems to make outgoing dial-up calls, must be established over *IT Security* approved *modem pools*.

7.1.9 No Release of Internal Network Configurations

The internal addresses, configurations, and related system design *information* for UBS networked computer systems must be hidden to the outside.

7.1.10 Classification of Network *Information*

Information regarding access to UBS computer and communication systems, such as dial-up modem phone numbers, is classified as "Confidential" an must be treated as

such.

7.1.11 *Authorization* for network services

Changes to network services provided on the UBS network must be approved by *IT Security* prior to their implementation and use.

7.1.12 Register of Connections

A register must be maintained which covers all categories of connectivity into or from the UBS network, including all hardware and software *IT assets* involved.

7.1.13 Protection of Network security Systems

Network security systems must be especially protected against internal and external intruders. Particularly the systems must be installed in a physically secured and access-restricted area.

7.2 Dial-Up Computer Communications

7.2.1 Direct Dial Connections

With the exception of portable computers and telecommuting computers, the use of local modems to establish direct dial connections is prohibited. All dial-up connections with UBS systems and networks must be routed through a *modem pool* which includes an approved *strong user authentication* security system.

7.2.2 Computer Modems

Modems connected to any *IT system* must not be left in auto-answer mode, such that they are able to receive in-coming dial-up calls.

7.2.3 Systems Accepting In-Coming Dial-Up Calls

Communications systems which accept in-coming dial-up calls must not be established unless these systems have first been approved by *IT Security*.

7.3 Remote Access

7.3.1 Equipment Compliance

Equipment supplied by UBS for *remote access* purposes must be compliant with the appropriate regulations for the country in which it will be used.

7.3.2 Denial of Unauthorized Activity

Attempts to execute transactions outside the scope of the remote connection must be blocked and an appropriate alarm must be raised. UBS's security measures must be such that, if necessary, UBS can interrupt or terminate the session.

7.3.3 Remote Maintenance

Remote maintenance connections for UBS *IT systems* must be disabled until the specific time as they are needed by the vendor or support staff. After use, these connections must be disabled immediately. Alternatively, remote maintenance connections must be established via outbound calls initiated by UBS personnel.

7.4 Electronic Mail

7.4.1.1 Use of Internal E-mail

E-mail must never be used for unencrypted *data* classified as "Confidential" or higher. *Data* classified as "Secret" must never be sent by e-mail regardless of being encrypted or not.

7.4.1.2 Use of External E-mail

E-mail messages routed over public networks must contain public *information* only, unless the contents are encrypted by *IT Security* approved methods.

7.4.2 Identity on Electronic Communication

Misrepresenting, obscuring, suppressing, or replacing an IT user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related *data* included with messages or postings must reflect the actual origin of the messages or postings.

7.4.3 Common Control *Procedures* for E-mail

E-mail users, when sending e-mail outside UBS, are bound by the same UBS security policies and *procedures* that control other forms of external correspondence such as paper, telephone and fax.

7.4.4 Forwarding Electronic Mail to an External Address

Unless the information owner/originator agrees in advance, or the *information* is clearly public in nature, IT users must not forward electronic mail to any address outside UBS's network. Auto-forward is prohibited.

7.5 Internet

7.5.1 *Data* and/or Program Downloading from the Internet

Data must only be downloaded from the Internet to UBS networks under the following conditions:

- All *data* are checked for viruses using an *IT Security* approved method and tools before they are installed on UBS systems.
- All *data* are business-relevant and appropriate, and are acquired and used in compliance with all UBS and legal requirements.
- Class exceptions may be granted by *IT Security* for controlled access to entities with whom UBS has an established *trust* relationship.

The Installation of software downloaded from the Internet must be subject to the standard software installation *mechanisms*.

8 Physical Aspects of IT security

8.1 Physical Access Security

8.1.1 Prevention of Unauthorized Access

Buildings which house UBS computers or communications systems must be protected with *physical security* measures that prevent unauthorized persons from gaining access.

8.1.2 Computer or Communications Systems In Locked Rooms

All security sensitive or critical computer, communications and infrastructure equipment must be located in locked rooms.

8.1.3 Printing of Confidential Output

Printers being used for printing *data* classified "Confidential" can be left unattended only if they are located in an appropriately *secure environment*. Printing *data* classified as "Strictly Confidential" or higher must always be supervised.

8.1.4 Supervision of Hardware Maintenance Personnel

Access to UBS IT equipment by hardware maintenance staff must be controlled.

8.2 Physical Security of IT Assets

8.2.1 Workstation Positioning

Workstations handling sensitive UBS *data* must be positioned so that unauthorized viewing of the screens is avoided. Proximity to external windows must be avoided.

8.2.2 Physical Storage of Electronic *Media*

All *data* storage *media* (such as hard disk drives, floppy disks, magnetic tapes, and CD-ROMs) containing non-public UBS *data* must be physically secured when not in use.

8.2.3 Use of *Transportable Computers*

Individuals in the possession of portable computers (laptop, notebook, palmtop) or other *transportable computers* or storage *media* containing non-public UBS *data* must not leave these unattended at any time unless the *data* has been properly safeguarded.

8.2.4 *Transportable Computers* on Airplanes

Individuals in the possession of portable computers (laptop, notebook, palmtops) or other *transportable computers* or storage *media* containing UBS *data* classified as "Internal Use Only" or higher must not check these computers in airline luggage systems. These computers must remain in the possession of the traveler at all times.

9 Personnel Aspects of IT security

9.1 IT security Awareness and Training

9.1.1 Awareness Program

There must be an ongoing awareness program in place to ensure that all IT-users understand how *IT security* relates to their functions.

9.1.2 Sufficient Resources to Address *IT security*

Management must allocate sufficient resources and staff attention to adequately address IT systems security.

9.1.3 Sufficient IT security Training Time

Management must allocate sufficient on-the-job time for employees to acquaint themselves with UBS IT security policies, *directives*, *standards*, *procedures* and related ways of doing business.

9.1.4 Attendance at IT security Class

Every IT-user must attend an IT security awareness class when they begin employment with UBS.

9.1.5 Central information board for *IT security* issues

A central information board containing *IT security* issues for end-users has to be established.

9.1.6 *Third Party* IT security Responsibilities

UBS's business partners, suppliers, customers, and other business associates must be made aware of their IT security responsibilities via specific language appearing in contracts which define their relationship with UBS.

10 Document and Media Security

The content of this chapter relates to storage and disposal of *media*. These subjects are covered elsewhere in this document.

11 Disaster Recovery and Business Continuity

11.1 Systems Design

11.1.1 Dispersion of Computer and Communication Systems

Computer and communications systems shall be geographically dispersed whenever possible.

11.1.2 Avoidance of Central Point of Failure in Networks

Management must design UBS communications networks so that no single point of failure could cause network services to be unavailable.

11.2 Contingency Planning

11.2.1 Business Continuity Planning

All business units must prepare, periodically update, and regularly test plans that will allow to continue business operation on a reduced level in case of *IT systems* being partly or entirely unavailable for various periods of time.

11.2.2 IT Contingency Planning

IT must prepare, periodically update, and regularly test a disaster recovery and emergency response plan that will allow:

- the continued operation of critical *IT systems* in the event of an interruption or degradation of service
- all critical computer and communication systems to be available in the event of a major loss

11.2.3 Segmenting *Data* Resources

IT Operations management must establish and use a logical framework for segmenting *data* resources by recovery priority. All departments must use this same framework when preparing *IT systems* contingency plans.

11.2.4 Level of Disaster/Emergency Support Levels

User department management and IT must determine and agree on the support levels that will be provided in the event of a disaster and/or emergency.
These levels must appear in contingency planning documents and service level agreements.

11.3 Back-Up, Archival Storage

11.3.1 *Data* Back-Up and Back-Up Frequency

All *critical data* resident on UBS *IT systems* must be periodically backed-up according business needs.

11.3.2 Back-Up *Media* in Separate Fire Zones

Computer and network back-up storage *media* must be stored in a separate fire zones from the machine producing the back-up. Fire zones vary from building to building, and are defined by Corporate Security.

11.3.3 *Data* Retention Period

Unless the type of *data* is specifically listed on the *Data* Retention Schedule, *data* must be retained for as long as necessary but for no longer. *Data* listed on the *Data* Retention Schedule must be retained for the period specified. Other *data* must be destroyed when no longer needed by an *IT Security* approved method with respect to the applicable laws.

11.3.4 Testing of Archival Storage Data *Media*

Critical data stored on computer *media* for a prolonged period of time must be tested regularly to ensure that the *data* is still recoverable.

12 Teleworking IT security Issues

Other issues related to teleworking are covered elsewhere in this document, particularly in Chapter "7, Communications and Network Security"

12.1 Equipment for Telecommuting

IT-users working on UBS business at alternative worksites must use UBS-provided computer and network equipment. An exception will be made only if other equipment has been approved as compatible with UBS *IT systems*, and IT security measures.

12.2 Changes of Computers Provided by UBS

Computer equipment provided by UBS must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without departmental management approval and *authorization* from *IT Security*. Any changes have to be done exclusively by designated UBS personnel.

12.3 Protection of UBS Property at Alternative Worksites

At alternative worksites, reasonable precautions must be taken to protect UBS hardware, software, and *data* from theft, damage, and misuse.

13 Outsourcing Aspects of IT security

13.1 No Degradation of *Trust*

Outsourcing of IT services to a third-party service provider must not introduce any degradation of *trust* unless it is formally accepted by IT and *IT Security*.

13.2 No Degradation of Security

Security must not suffer for any reason (e.g., cost reduction, better cost visibility, access to expertise, focus on mainline business issues, etc.) by the outsourcing of IT services. Alternatively, an increased risk must be formally accepted and born by the IT asset owners.

14 Change Control

14.1 Feedback

All IT users and other reader of this document might feel free to give feedback and proposals for amendments to the author(s) or the issuing bodies.

14.2 Changes to the Security Policy

The IT security *functional policies* are established by IT Security Heads and are then ratified by UBS's IT Committee and UBS Divisional Executive Board as appropriate.

The IT security *functional policies* will be reviewed as often as necessary but no less than annually. Additional functional policy statements will be issued as needs arise, and will be incorporated into the IT security *functional policies* document during renewal periods.

15 Glossary

15.1 Terms

The terms laid out below are focussed on *IT security* concerns. For some few general terms, the meaning of their use in this document is explained too. Further general Information Technology terms can be found on the BankWeb in the "Technical Glossary" (http://bw.ubs.com/help/glossary/glossary.htm).

Term	**Explanation**
Access control	Depending on the context, access means, in a general sense, *authorization authentication and privilege control*, but also the process of granting or denying a subject access to objects
Asymmetric algorithm	*Encryption/authentication* algorithm with private (*decryption*/signing) *keys* and public (*encryption*/verification) *keys* and the property that a *private key* cannot be derived from its corresponding *public key*
Authentication	(see entity authentication) (see message authentication)
Authorization	The administrative process of assigning rights to a subject
Availability	The property that *data* is protected from loss and ensuring that it is available to authorized users in the requested form whenever and wherever required
Certificate	The *public key* of a user together with related user *data* signed by a Certification Authority
Certification authority (CA)	A *trusted* entity in a network with tasks similar to a notary: registers new users and certifies their *public keys*
Ciphertext	Non-Intelligible text or signals which can be read or acted upon only after the application of an appropriate *decryption*
Confidentiality	The property that *information* is not made available or disclosed to unauthorized individuals, entities or processes
Credential	An object containing security *information* about a subject.
Critical data	*Data* to be prevented from loss or unavailability for a predefined period of time, e.g. *data* classified as "Max. 1-hour unavailability allowed" or less
Cryptographic key	A sequence of symbols or bits that controls cryptographic operations like *encryption, decryption*, *authentication* or signature generation
Cryptography	The discipline which embodies principles, means and methods for the transformation of *data* in order to hide its content, prevent its undetected modification, prevent its unauthorized use, or guarantee its authenticity
Data	Refers to all *information* which can be electronically stored, processed and transmitted. Data may be processed in internal main memories,

	stored on electronic *media* , and transmitted by networks
Data classification	The assignment of *information* or a document to a category on the basis of its sensitivity to disclosure or to modification or destruction or to its legally binding force
Data integrity	The property that *data* has not been modified in an unauthorized manner
Data protection	Requirements for the handling of personal *information*, e.g. regarding accuracy and *confidentiality*
Decryption	The inverse process of *encryption* (see cryptography)
Demilitarized zone (DMZ)	Protected network segment within *firewall* infrastructure
Digital signature	A checksum based on asymmetric cryptographic algorithms to verify the originality of *data*. The asymmetry yields *non-repudiation* by the sender because not even the receiver can forge the signed *data*
Directive	An IT security directive consists of required actions to be taken and directions to be followed in implementing the current IT security *functional policies*. A directive is well defined, feasible, and executed in the manner specified. It can be tested for compliance. A directives will change as the environment changes and/or new methodologies become available
Dual control	Dual control means that two people must be simultaneously present for an important activity to be accomplished
Encryption	The cryptographic transformation of *data* to produce *ciphertext* (see cryptography)
Entity authentication	The confirmation that an entity in an association is the one claimed
Extranet	A logically separated extension of the UBS network to all entities that UBS does business with: employees, business customers, prospects, partners, consultants, and others
Firewall	A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed a security check (such as providing a password or conforming to a previously authorized source or protocol)
Firewall gateway	System separating closed corporate network from the outside world allowing only predefined *data* exchange
Functional policies	The IT security *functional policies* cover all of the management decisions, intentions, definitions and rules relating to *IT security*
Guidelines	IT security Guidelines are recommended actions and help in deciding the best course of action to follow in implementing current policies. Guidelines should always be considered in the context of the best business practices. Guidelines will change as the environment changes and/or new methodologies become available.
Identification	The process of recognizing an entity (e.g. user or process) based on its unique distinguished name
Incident	See security incident

Information	The meaning assigned to *data* by means of conventions applied to that *data*.
Information Security Policy Statement	Sanctioned at Board level for application throughout UBS, defines principles and responsibilities which constitute *IT security* within UBS and provides the foundation for its day-to-day execution
Integrity	The completeness and accuracy of data assets
IT asset	IT assets are electronically stored data assets including the physical and logical means by which the *data* is stored, processed and transmitted
IT process	I processes are functions, *procedures* or activities by which electronically stored data assets are processed and transmitted
IT Security	Organizational unit within UBS IT organization that develop, implement, administer, and review the protection of *IT assets* and monitor compliance to IT security *functional policies*, directives and *standards* through the UBS IT security programs.
IT security	Information Technology Security is the provision of organizational, technical and social measures to safeguard *IT assets* against unauthorized access, damage and interference - both malicious and accidental
IT system	Depending on the context , IT systems means all computer and communication network facilities, including hardware and operating system software, or application and/or infrastructure software running on them, or both, processing and/or transmitting *data* and *information*
Key	(see cryptographic key)
Key distribution	The secure transportation of *cryptographic keys* to their destination
Key management	Encompasses all activities and operations with *cryptographic keys*: generation, storage, distribution, deletion, archiving and application
Logging	Tracing and archiving operations in a system for later retrieval or analysis
Malicious code	Intentionally written code which may cause reading out or loss of *data*, or more generally, harm to *IT systems*. Malicious code can hide within programs, scripts and macros. Common forms are: Viruses, Worms, Trojan Horses, Logical Bombs, etc. Distribution of malicious code mostly happens via e-mail or through unauthorized downloads from the internet but also by data carrier exchange as floppy disk, CD-ROM etc.
Masquerade	The pretence of a false entity (e.g. impostor) to be a different and valid entity (e.g. user)
Master key	A *cryptographic key* used to encipher application *keys*, e.g. data-encrypting or file *encryption keys* (see hierarchical *key management*)
Mechanism	Security mechanisms are all kind of technical and/or organizational security measures
Media	Transportable computer-readable storage media such as magnetic tape, floppy disk, CD-ROM and others
Message authentication	The confirmation that the source and contents of a message is as claimed
Modem pool	Collection of several modems, which are managed all the same way

Non-public data	*Data* classified as "Internal Use Only" or higher
Non-repudiation	The property that an entity cannot deny an action, i.e. legally binding assurance that transmitted *data* has been both issued and received by the correct, authorized persons
One-time password	Password that can be used only once (e.g. for *strong authentication*)
One-way function	A mathematical transformation for which no inverse function exists or the inverse function cannot be computed in reasonable time
Physical security	The measures used to provide physical protection of resources against deliberate and accidental threats
Plaintext	Intelligible text or signals that have meaning and which can be read or acted upon without the application of any *decryption*
Private key	The secret part of the key pair used in asymmetric *encryption* schemes (see *asymmetric algorithm*)
Privilege control	The process of granting or denying a subject access to objects
Procedure	Security procedures are organizational security measures
Public key	The public part of the key pair used in asymmetric *encryption* schemes (see *asymmetric algorithm*)
Public key encryption	Encryption method using *asymmetric algorithms* requiring a *public key* for encryption and a *secret key* for *decryption*
Remote access	Remote access denotes any usage of the UBS network which comes from outside UBS's controlled and protected environment. Remote access connections include connections to mobile employee laptops, employee dial-in connections from their residence, customer connections and vendor connections. Remote access also includes all dial-out modem connections established from any machine off the UBS network. Common to virtually all remote accesses is a reduced or uncertain *trust* level at the remote end
Risk Management	Managing the security risks imposed by the operation of any *IT system* is necessary for two distinct reasons: • linking the investments into IT security measures to UBS's investment policy • contribute the security risks to the bank's overall *risk management* UBS's approach to IT security *risk management* is an iterative process consisting of the 4 activities • Risk Identification • Risk Assessment • Risk Mitigation • Risk Monitoring
Role	Set of applicatory rights required in order to do a specific job
Role-based access control	Role-based *access control* allows the creation of *roles* for which appropriate privileges are explicitly assigned. Individual users are enrolled in appropriate *roles* from which they inherit these privileges
Screen saver	A computer program that automatically blanks and/or locks the screen of a computer monitor or terminal after a certain period of inactivity

Secret key	The *cryptographic key* used in symmetric encryption schemes or the private part of the key pair used in asymmetric encryption schemes
Secure environment	UBS controlled premises, i.e. rooms or buildings to which UBS controls access
Security incident	An IT *security incident* is defined as any unauthorized action taken on UBS *IT assets* which intentionally reduces, compromises or threatens the *confidentiality*, *integrity*, *availability*, recoverability, or *non-repudiation* of the *data* or *IT systems* themselves. This includes, but is not limited to, the following: • Removing or bypassing existing protection and control *mechanisms* • Using or misusing control *mechanisms* to gain or grant unauthorized access or system privileges • Reading, copying, modifying, or deleting *data* by an individual or program not authorized for such actions • Abusing privileged access in order to monitor or impersonate another IT user, or reading that individual's private *data* without *authorization* • Attempting to explore or test for security vulnerabilities in *IT assets* when not authorized to do so
Sensitive data	*Data* to be prevented from disclosure to unauthorized individuals, i.e. *data* classified as "For Internal Use Only" or higher
Separation of duties	Means that an important activity to achieve an objective is separated into two or more tasks performed by two ore more different individuals to supervise each other
Simple authentication	Mechanism for *entity authentication* using password to confirm the identity
Smartcard	Security module used for *user authentication* with the size of a credit card incorporating a processor and memory for using and storing secret *data* (e.g. *keys*) and executing algorithms
Standard	An IT security standard function, product and process is a current specification, tool or *procedure* to be used in implementing the current policy. This standard function, product or process is intended primarily for IT providers and contain the approved IT security methodologies for UBS's use
Strong authentication	*Entity authentication mechanism* that guarantees that the *authentication* process cannot be faked using *information* transmitted over a network during a previous *authentication* process. Achieving this goal requires *authentication* protocols based on *cryptography*. Normally they are based on the challenge-response principle (see challenge-response *mechanism*)
Symmetric algorithm	*Encryption* algorithm with the property that *keys* for *encryption* and *decryption* are the same and therefore need also the same level of protection
Tamper protection	Physical protection of secret *data* (*keys*) which allows detection of intrusion or even destroys the secret *data* if tampering is detected
TEMPEST	"Transient electromagnetic pulse emanations standard" - A secret NATO standard for the limitation of electromagnetic radiation from

	equipment, i.e. for avoidance pick up *plaintext* radiation and recreation screen images by an outsider
Third party	External partners like vendors, data feed provider external supporter/developer.
Transportable computers	All portable computer devices such as laptops, notebooks, palmtops, and other that can store and process *data*
Trust	Element x trusts element y for some classes of operation in the context of a security policy if and only if element x has confidence that element y behaves in a well defined way that does not violate the security policy
Trust chain	A set of *trusted systems* which are linked into a request chain
Trust domain	A set of *trusted systems* which are managed by the same authority and adhere to the same security policy
Trusted environment	The set of all *trusted systems* on a private network
Trusted path	A communication path between two entities which is believed to be authentic and conserves *confidentiality* and *integrity*
Trusted system	A system that is *trusted* to comply with the UBS IT security framework
Tunneling	Architecture that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme
User authentication	*Entity authentication* between user and server/service
UserID	A unique name/number identifying a unique person or process
Virtual private network (VPN)	Exchange of network traffic in a secure manner, even if *data* flows across a public network. With *encryption* (*tunneling*, encapsulation) of network traffic, *data* is exchanged almost as if the traffic would be transmitted over a private network