26th. November 2009

IT security policy v. 3.0.16 for the Danish Technological Institute

Company	Danish Technological Institute
Address	Gregersensvej 1 A
Zip City	DK-2630 Taastrup
Telephone	+4572203407
Fax	04572202019
Policy Name	IT security policy v. 3.0.16
Created	9/8/2009
Last Edit	9/8/2009
Last Edit By	Peter Hjortshøj

Selection Criteria

Policy Responsible	ALL
Porc Responsible	ALL
Auditor	ALL

Based on the Danish Standard DS484, 2005

Index

1 INTRODUCTION

1.1 Why information security

IT security constitutes a necessary part of the Danish Technological Institute's protection of business assets and activities in line with the general security and protection against burglary, fire and the like.

1.2 This IT security policy and DS 484

This IT security policy has been drawn up on the basis of the Danish Standard for information security DS484 (2005) which is a continuation of the British BS7799. We have chosen those parts of the standard which are relevant for this company's business and activities and we have weighted criteria such as business sensitivity and personal sensitivity in our data and in areas such as confidentiality, integrity and access to the company's systems and data. The level of detail is relatively high as the topics have to be measurable.

Statement:

The table of contents (indexation) in this IT security policy has been reproduced with permission from Danish Standard on: 16 August 2006.

1.3 Assessment of security risks

Assessment of security risks must always be based on the Danish Technological Institute's situation, position in the community and the interest of the outside world for the products. The security level must be set at a level which on the one hand protects the company's assets and activities sufficiently against interruptions and data loss, and on the other hand does not prevent or limit the employees' possibility more than absolutely necessary of carrying out their work and showing creativity. As a basic principle, the company trusts the employees and supervision is only exercised where it serves a purpose.

1.4 Choice of security and protection measures

Based on risk and consequence assessments, it will be decided which security measures are to be implemented. The choice lies between preventive or corrective activities. If the accident should occur nonetheless, the choice lies between having a contingency plan and having accepted the risk and the consequence beforehand. The company's insurances must naturally be in place in all areas.

1.5 The company's specific security guidelines

The specific security measures must be carried out in the whole organization. There will be a need for solutions for physical security (the building, supplies), the technical (hardware, software) and the human side (training, procedures).

Continuity in the security policy will be ensured by cooperation between Joint Functions. The work will be monitored by the Management and the IT Executive Committee.

1.6 Exemption from the IT security policy

Where existing systems do not live up to parts or the whole of the present IT security policy, there may be a need for exemptions. Ascertained deviations must be registered and it must be decided in how far the systems are to be isolated, updated or phased out as soon as possible.

Exemption from this IT security policy must be approved by the IT Manager or the IT Executive Committee.

1.7 Risk management

Risk management is predefined in the company's business procedures and processes under line responsibility, so that the topic is treated where and when it is relevant. The company must carry out overall risk and consequence assessments periodically of building, technology, applications, processes etc.

The aim is partly to ensure that the necessary security level is adjusted in step with changing needs, and partly to keep an eye on the company's most operationally crucial systems.

1.8 Contingency plan

As a result of the risk and consequence analysis, the Danish Technological Institute's most operationally crucial systems will be defined and contingency plans will be drawn up for these. The operational importance of the systems reflects at the same time an order of priority for where the resources are to be concentrated if errors or accidents occur on a broader front.

The contingency plan must be drawn up on the basis of the time perspective: How long the company can manage without access to a given system, which operational costs it will inflict on the company, which resources are necessary and how long it will take to recreate a reasonable operational level.

1.9 How has the IT security policy been drawn up

This IT security policy has been drawn up on the basis of eligible texts in "Policy Enforcer".

The texts have been discussed in a series of meetings in which the Management, managers in charge of Staff, Finances, IT and others participated.

1.10 Relevant legislation

In connection with IT security, the following legislation, rules and branch regulations are relevant for the company.

Law on employment contracts
Archives law (public companies)
The Accounting Act
Law on E-trade
Law on electronic signatures
Marketing Practices Act
Copyright Act
Law on Personal Data
Criminal Code
TV Surveillance Act

1.11 Responsibility for maintenance

The IT Manager must ensure, on an ongoing basis, that the IT security policy complies with current legislation and that it covers the risks and consequences which can damage the company's goals and business intentions.

The IT security policy must be reviewed at least once a year.

1.12 Area of validity and scope

The IT security policy is in force all over the company, at home and abroad, to be used in the company's IT domicile, branches, during journeys and in connection with working from home.

Relevant parts of the IT security policy apply for cooperation partners in their work for the company, from the company's addresses or from the partners' addresses.

1.13 Date and period of validity

This IT security policy is valid from 1 September 2009 and until a new version is available.

2 THE COMPANY'S IT SECURITY POLICY

2.1 The Company's IT security policy

Maintaining and expanding a high level of security is an important prerequisite for the Danish Technological Institute's credibility both nationally and internationally.

In order to maintain the Danish Technological Institute's credibility it must be ensured that information is treated with the necessary confidentiality and that approved transactions are treated completely, precisely and punctually.

Next after the employees, IT systems are considered as the Danish Technological Institute's most crucial resource. Importance is, therefore, attached to reliability, quality, compliance with legislative requirements and to the systems being user-friendly, i.e. with no unnecessarily difficult security measures.

An efficient protection against IT security threats must be created, so that the image of the Danish Technological Institute and the safety and working conditions of the employees are ensured in the best possible way. All circumstances must be weighed against the business risk, so that security measures do not become an unnecessary hindrance for carrying out the work and attending to customers.

Protection must be directed against natural, technical and also man-made threats. Each person is considered as being a possible cause of a breach of security; i.e. no group of people will be above the security regulations.

Therefore, the aims are to:
ACCESSIBILITY – attain a high level of reliability with high uptime percentages and minimized risk of large break-downs and data loss.
INTEGRITY – attain correct function of the systems with minimized risk of manipulation of and errors in both data and systems.
CONFIDENTIALITY – attain confidential treatment, transmission and storing of data
AUTHENTICITY – attain mutual security around the parties involved
IRRETBUTTABILITY – attain security for mutual and documentable contact

3 ORGANIZING IT SECURITY

3.1 Internal organizational conditions

The management of the company is responsible for company information assets being managed in accordance with current legislation and in addition that they are sufficiently protected in a business context.

3.1.2 Distinction of function

Access to and management of data should only take place on the basis of current needs and in such a way that there is a clear distinction between development, maintenance, testing and operation.

Similarly, there should be a clear distinction between the planned, executive and monitoring functions in so far as it is organizationally possible.

3.1.3 System and data owners

Every IT asset (data register, program, physical unit and other) must have a named owner who is responsible for acquiring, maintaining and operating the asset.

For example, the system and data owner lays down rules for access, rights, back-up, storage, transport etc.

3.1.4 User administration

User administrators have been appointed for all systems to carry out the physical data entry of user profiles, rights etc. on the basis of orders from those persons who can assign and approve rights.

For central systems, all user operations are handled in writing via Brugeropret (Create User).

3.1.5 IT operation

The IT operation unit is responsible for all security rules and procedures being followed in daily operations and for problems and errors being detected, corrected and reported.

The IT operation unit is part of the ongoing work (proposals and implementation) with improving security measures (procedures, methods, products).

3.1.6 User responsibility

Every user of company IT systems is responsible for complying with current policies and rules in the area.

The user must report to the nearest manager or to the person responsible for IT regarding incomprehensible or ‘strange’ occurrences while using the IT systems.

Every user is responsible for acquiring the necessary training and knowledge in order to be able to live up to the function in question and to operate the IT systems involved.

3.2 External organizational conditions

3.2.1 Contact to authorities

The management secretariat keeps records of the most important contacts with public authorities in relation to the company's security and activity. This includes:

Fire
Burglary, vandalism
IT security breaches
Environment

3.2.2 Cooperation with suppliers, consultants and others

Via membership of relevant associations and in cooperation with relevant suppliers, the organization will ensure access to updated knowledge about security, risks, methods and tools of protection.

3.2.3 IT security in relation to customers/customer service

Security must be built up in such a way that no form of confusion can occur with customer information and orders, or loss and manipulation of information.

Security and safety measures must be established in such a way that they do not inconvenience or delay the Institute's customers significantly, whether the customers are personally present at the Institute or whether they use machines, websites or similar service facilities.

3.2.4 Professional cooperation with groups and organizations

Security must be built up in such a way that no form of confusion can occur with information and orders from cooperation partners and other organizations, or loss and manipulation of information.

Security and safety measures must be established in such a way that they do not inconvenience or delay the Institute's customers significantly, whether the customers are personally present at the Institute or whether they use machines, websites or similar service facilities.

3.3 Coordination of IT security measures

3.3.1 Line organization

It is the job of the line organization to plan and execute the daily business tasks under due consideration to the current rules and guidelines in this IT security policy with underlying procedures.

3.3.2 IT security coordination

The IT Manager has the total responsibility for the overall coordination of security and must call the IT Executive Committee to meetings and collect, process and present status information for the committee.

With regard to assignments, the IT Manager refers directly to the Management.

3.3.3 IT Security Committee

The IT Executive Committee is the IT Security Committee of the Danish Technological Institute and consists of representatives from the Management, the IT-management and selected system owners (crucial systems). The IT Executive Committee will assess the Institute's security and safety on the basis of status reports from the IT Manager. The committee can ask for information on new risks, security methods etc. and decide which security measures are to be implemented.

3.4 The Company's IT assets

3.4.1 Registration of information assets, data classification etc.

The Institute's data registers (files, data bases etc.) must be registered in a joint registration system stating ownership and be classified as a basis for correct data security and protection.

3.4.2 Registration of system assets, systems

All systems (operative systems, office systems, tool programs etc.) must be registered in registration systems stating use, ownership, license numbers, version numbers etc.

The registration must be continuously updated.

3.4.3 Registration of physical assets, marking etc.

All physical units (servers, work stations, portable computers) must be registered in registration systems stating serial numbers, ownership and date of initial operation.

The registration must be continuously updated.

3.4.4 Ownership

All physical units (machines, programs, applications, data) plus important business processes must have an owner who is responsible for acquisition, maintenance, access, operation etc.

4 EMPLOYEES AND IT SECURITY

4.1 Before appointment

4.1.1 Clearing of applicants

The applicants' background and any references should be examined on the basis of the position in question to be filled.

4.1.2 Confidentiality and secrecy declarations

Every employee is bound by a confidentiality obligation with regard to various business matters according to current legislation.

All employees must sign a special Secrecy Obligation in connection with their appointment.

4.2 During employment

4.2.1 Physical keys, ID cards, tokens etc.

Physical keys, access cards, tokens and the like to the Institute and its IT systems are allocated on the basis of 'roles'. The allocation must be registered centrally and kept up-to-date in step with changes of premises and in connection with new appointments, moves and termination of employment. The employee must sign a receipt for the effects. The allocations must be revised periodically.

4.2.2 Handling company IT assets

It is the personal responsibility and duty of each employee to operate the IT equipment at their disposal according to the guidelines, rules and regulations given by those responsible for systems/IT, suppliers and manufacturers. The employee must immediately report problems and errors to the nearest manager or to the person in charge of IT systems.

Only persons in charge of systems may make changes in the system setup and machinery or try to bypass security systems in a test phase.

4.2.3 Personal password (code word) and other codes

Personal passwords (code words) must be changed periodically (every 3rd month). The new password must be complex, unique, differ significantly from the one previously used and may not be systematic.

The password will be given to the employee upon application to IT. The password must be reset and corrected at the first login.

Users may not store their password electronically, note it down or pass it on to others.

If the same password is used in several systems, the password must be changed simultaneously in all systems. The password and other codes may not be passed on to others.

4.2.4 Employee training – in relation to security

It is the responsibility of each manager that the employees attain sufficient understanding of the Institute's IT systems through formal education and daily training, so that these systems are handled and operated correctly to ensure that data is always correct and valid, alternatively that errors can be detected.

All employees must be familiar with the Institute's IT security policy, relevant security rules, rules for reporting and the consequences of any breach of these.

4.2.5 The employees' awareness in relation to security

Employees must be aware of deviations from the normal use of the Institute's IT systems: Unknown e-mails, e-mails from unknown sources, e-mails with strange headings, double sign-on, websites, e-mails or telephone calls which attempt to entice identities, codes and the like from the user or other occurrences on the computer which deviate from the way in which the system usually reacts.

Deviations must be reported immediately to IT.

4.2.6 Key employees – a management responsibility

Every manager must ensure knowledge-sharing within his/her area of responsibility. The department must be organized in such a way through activity assignment, training and project work that the risk of 'key employees' arising is limited.

For the sake of security, business crucial information must be registered (on paper or computer) and there must be procedures for ensuring the maintenance, actuality and validity of the information.

4.2.7 E-mails which are binding for the company

Binding agreements for the Institute must be handled in writing and under conditions in force for entering into agreements.

If a written agreement is sent via e-mail, the Institute's digital signature should be used for secure identification to the recipient. The nearest manager should always receive a copy.

4.2.8 E-mail communication in general

The Institute's e-mail system may not be used to propagate material of an offensive, religious or political nature, and the employees are not permitted to send SPAM, such as jokes, chain letters and the like. A breach of these rules can have consequences for their employment.

Unsolicited promotional messages, special offers, newsletters or similar material may not be sent in the form of e-mail to customers and partners without their prior acceptance or approval.

Internal mail may not be forwarded to private e-mail addresses and the like outside the Institute.

It is not possible to delete e-mails at the Danish Technological Institute.

4.2.9 E-trading which is binding for the company

E-trading (electronic purchasing) may only be carried out on behalf of the Institute by employees with special authorization.

4.2.10 Use of Internet-based services

All use of Internet-based services, such as communities, social networks, file-sharing and other group-based services must have prior approval by the IT Manager.

Private and work-related spheres must be kept strictly separate.

4.2.11 Employees' use of publicly accessible computers

Employees' use of publicly accessible PC equipment (e.g. at airports, internet cafés, hotels etc.) for writing, internet searches, e-mails and the like must be limited.

Any such use should not include confidential or personal sensitive information. Personal names and the like which are clearly identifiable must be blurred. It must be ensured that any company data on the external equipment is deleted before leaving the equipment.

4.2.12 Private use of the company's Internet connection

Private use of the Internet from the Institute's computers must be limited during working hours. This includes private use of services such as communities, social networks, file sharing and other group-based services.

The Institute offers free access outside normal working hours, but with the restrictions of use stated in other sub policies.

4.2.13 Private use of the company's e-mail facilities

Private e-mails may only be sent to a limited extent on company e-mail systems.

E-mails with attached documents can be rejected. Private e-mails should be marked PRIVATE. All e-mail traffic is registered with backup, and can be accessed if technical problems arise.

Internal mail may not be forwarded to private e-mail addresses and the like outside the Institute.

4.2.14 Private downloads and copying of music, games, pornography etc.

Institute computers may not be used for downloads and copying of games, unlicensed music and software or materials of an offensive, religious or political nature.

Pirate copying may result in consequences for the employment of the person in question and in special cases to a police report.

4.2.15 Private e-trading from company systems

Private e-trading may only be carried out from the Institute's IT systems if the transaction in no way can compromise or bind the company.

4.2.16 Use of cameras and mobile cameras in the company

Neither employees nor guests are permitted to record any kind of photos in the company area without written permission from the company management. All types of cameras must be turned off inside the company area. If permission is given, the departmental manager is responsible for which parts of the company may be photographed.

4.2.17 Use of TV surveillance in the company

TV surveillance can be used in connection with surveillance of the normal access roads to the company and in particularly sensitive areas and departments for ongoing monitoring of unlawful access and inappropriate behavior. The employees must be informed of this and the surveillance must be signposted.

The tapes will be stored and kept for a longer fixed period for use in case of police investigation after which they will be re-recorded or deleted.

Storing, deleting and discarding must follow the company rules for deleting data carrying media.

4.2.18 Use of sound recordings in the company

Telephone conversations from the Institute's telephone systems are not recorded without prior agreement with the employees in question.

4.2.19 Use of remote devices

The use of remote devices may only take place after acceptance from the user. Remote devices must be approved by IT.

All connections with remote devices – and attempts at connection – will be logged with information on the access taking user/pc as well as the point in time of connection and disconnection.

4.2.20 Remote access

VPN may only be used by employees at the Danish Technological Institute with allocated initials. Installation of VPN software may only be carried out by IT on equipment approved by IT (where the other security requirements are met).

If a VPN access is not used for three months, it will be closed. VPN access will be reopened by IT based on a check of the employment relationship.

4.2.21 Inactivity

Inactivity for 3 months will result in blocking of:

- Network accounts and VPN. Can be reopened by IT based on a check of the employment relationship.
- Network connection. Reopened by contacting IT.
- PC or other hardware. Reopening of access can only take place after the equipment has been updated.

If the employee does not receive wages for three months, the network accounts will also be automatically blocked.

4.3 After termination of employment

4.3.1 Transfer of data and ownerships upon termination of employment

If an employee resigns and terminates employment on his/her own initiative or if he/she is dismissed by the company, the nearest manager must ensure that data ownerships and data are transferred to other employees.

The transfer must begin immediately after notice is given.

Electronic mail which is received for the person who has left the employment will be delivered to another employee's internal mailbox after termination of the

employment. Full access to the mailbox belonging to the person whose employment has been terminated can only be allocated after written approval from the Personnel Manager or the Management with a subsequent report in Brugeropret.

Any request for an extension of network access after the date of termination of employment (winding-up activity) must be approved by Personnel and reported in Brugeropret with a new final date.

4.3.2 Withdrawal of IT rights upon termination of employment

If an employee gives notice or is given notice by the Institute, the nearest manager must assess the risk of the employee continuing to keep his/her IT rights until the date of termination.

All access to the Institute's systems will be closed for the person in question at the latest at the end of the last working day.

The telephone will be closed or referred to another number on the day of termination.

Persons whose employment has been terminated will be removed from the Institute's address list at the latest by the next working day.

4.3.3 Returning borrowed IT assets upon termination of employment

Upon termination of employment the employee must return all borrowed IT assets (ID cards, tokens, mobile phones, computers, routers etc.) at the latest by the last working day.

If the company dismisses the employee, the nearest manager must assess the need for an earlier withdrawal of the effects.

PC's, mobile phones, and other data carrying media must be handed in to IT for cleaning before they are passed on to another employee. Data carrying media which have belonged to managers must be destroyed by IT. Persons leaving employment cannot take over the equipment. Deviations from this must be approved by the Personnel Manager or the Management.

4.3.4 Withdrawal of IT rights, assets etc. in cases of expulsion

If an employee is dismissed and expelled, various accesses to the Institute's IT systems will be closed for the person in question immediately after expulsion. Borrowed IT assets (ID cards, tokens, mobile phones, computers etc.) will be withdrawn immediately.

If the expelled person has important effects at his home address, the nearest manager must assess the need for demanding that the effects are returned immediately or collected from his/her home. The Institute will issue a receipt for the transfer. The

employee's computers and data files will be gone through as soon as possible and relevant content will be transferred to other employees.

The nearest manager is responsible for the activities.

PC's, mobile phones, and other data carrying media must be handed in to IT for cleaning before they are passed on to another employee. Data carrying media which have belonged to managers must be destroyed by IT.

5 SECURITY, GUESTS AND COOPERATION PARTNERS

5.1 Permanent daily partners

5.1.1 Cleaning staff

Cleaning in IT and technology facilities must be carried out by permanent (and cleared) persons who have been given special guidelines and instructions. IT must ensure that the cleaning staff is familiar with relevant security arrangements and rules. In especially sensitive areas the cleaning must be carried out under supervision of an employee from IT.

5.1.2 Workmen

Workmen may only carry out work in IT and technology facilities if the purpose, scope and times of the work are known and approved by IT service.

Special measures must be taken to avoid operational breakdowns caused, for example, by electrical failures (consequences for IT equipment and alarms), vibrations, dust, smoke, moving equipment and disconnection of equipment. When using welding equipment, flammable chemicals and the like, special safety precautions must be taken.

The workmen must ensure that no other unauthorized persons have access to the area and they must inform IT when work will start and end each day.

The workmen must know who to refer to if any doubts or problems occur while they are working.

5.1.3 Goods suppliers

Suppliers of IT materials or other technology may only have access to the Institute's IT and technology facilities after arrangement and only accompanied by trusted employees from IT.

5.2 Permanent IT partners

5.2.1 System consultants

Permanent system consultants may be given access to the company's IT resources (offices, machines and systems) to the extent necessary for carrying out the assignment. Access and rights must be approved by the Systems Manager and the IT Manager. The allocated access is subject to periodical review.

If it is necessary to connect to the Institute's IT systems from outside, access may only be given for one session at a time under the surveillance of the Systems Manager. The Systems Manager is responsible for the consultants being familiar with the Institute's IT security policy and rules and that these are adhered to.

5.2.2 Machine technicians

Machine technicians from permanent cooperation partners whose identities are known have the same access to the IT and technology facilities as employees from IT. The allocated access is subject to periodical review.

No unknown technicians who have been called in may have access to the Institute's IT and technology facilities without presenting personal identification with name and company name. The work assignment and period must be known.

Unknown technicians must be accompanied by an employee from IT.

If it is necessary to connect to the Institute's IT systems from outside, access may only be given for one session at a time under the surveillance of the Systems Manager.

5.2.3 System developers

External system developers who need access to the Institute's systems must be cleared and approved by the Institute.

Access and rights will be allocated in proportion to what is necessary to carry out the assignment. Access and rights must be approved by the Systems Manager and the IT manager. The allocated access is subject to periodical review.

The developers must be familiar with the Institute's IT security policy, rules for handling the Institute's data, reporting etc.

If it is necessary to connect to the Institute's IT systems from outside, access may only be given for one session at a time under the surveillance of the Systems Manager.

5.3 Periodic guests

5.3.1 Sales representatives

External sales representatives may normally only move around at the Institute accompanied by an employee.

Guests are not permitted to use the Institute's networks (Lokanet and Labnet), but may use a cabled guest net (blue marking) or guest account (issued for 8 hours) on the wireless network. Guest accounts can only be issued personally by employees of the Institute.

5.3.2 External conference participants

External conference participants may only move around at the Institute accompanied by an employee, alternatively be registered on arrival.

Guests are not permitted to use the Institute's networks (Lokanet and Labnet), but may use a cabled guest net (blue marking) or guest account (issued for 8 hours) on the wireless network. Guest accounts can only be issued personally by employees of the Institute.

5.3.3 Temporary assistants

Temporary assistants and replacements may not normally have access to the Institute's IT and technology facilities or the like.

Access to use of the systems must be restricted to those systems which are necessary for carrying out the functions. Access must, if technically possible, be restricted with date and time interval.

The nearest manager is responsible for the temporary assistant being familiar with the Institute's security policy and rules for the area. In special cases it may be necessary to clear the temporary assistant. The allocated access is subject to periodical review.

5.3.4 Trainees

Trainees may not normally have access to the Institute's server facilities, technology facilities or the like. Access to use of the systems must be restricted to those IT systems which are necessary for carrying out the purpose of the traineeship. Access must, if technically possible, be restricted with date and time interval.

The nearest manager is responsible for the trainee being familiar with the Institute's security policy and rules for the area. In special cases it may be necessary to clear the trainee before access to the company is given. The allocated access is subject to periodical review.

6 PHYSICAL SECURITY, PROTECTION AND CONTROL

6.1 Conditions for buildings

6.1.1 The company's peripheral protection

The Institute's outer areas must be laid out in such a way as to ensure against unauthorized access and at the same time monitor the access and movements of company guests.

6.1.2 Protection of the company buildings

The buildings must be protected in such a way as to restrict the opportunity for unauthorized physical entry, theft, damage and vandalism in areas where theft or damage would entail great inconvenience and costs.

Preventive protection (locks, bars, protective film and other) should be supplemented with surveillance and alarm systems with direct contact to a security center.

6.1.3 Access to the company building(s)

Access to the Institute for guests and employees is through the main entrances of the Institute.

Mail and goods must be delivered directly to the relevant functions and areas. Other doors are protected and marked as emergency exits.

6.1.4 Access to IT and other technology facilities.

Access control to server facilities must be protected with an electronic locking system which can monitor and register access. Access must be based on a 2 factor technology. Server facilities must be divided into zones and have video surveillance, and allocated access must undergo periodical review. Employees from IT or employees appointed by IT have access according to needs. Zones with operational servers may only be entered by IT employees, and relevant technicians, consultants, workmen and cleaners only have access accompanied by employees from IT.

Other technology facilities/cabinets must be securely locked with a key system administered by IT and have video surveillance. Access keys are issued by IT.

6.1.5 Access to and protection of IT offices

Offices which are used by IT employees and where spare parts are kept, software packages etc. must be protected against unauthorized free access and against theft.

Doors must be locked when the rooms are not manned. Effects of special interest for thieves and media with sensitive information must be stored in locked units when not in use.

Only relevant materials may be present during conferences and visits (Clean-desk-policy).

6.1.6 Protection of work from private homes

As a basic principle all work with the Institute's IT systems and data from employees' private homes are subject to this IT security policy.

If a private computer connected to the company is used, then data may not be transferred to the private computer, neither by file transfer, attached to an e-mail nor in any other way.

The Institute's data must be treated and handled on the basis of their sensitivity and with special attention to rules for discarding data carrying media, including paper print-outs.

6.1.7 Access to and protection of conference and teaching facilities

The Institute's conference and teaching facilities can be used freely by the Institute's employees. The conference host is responsible for the movements of external participants in the area.

6.1.8 Access to and protection of common areas

Customer areas should be isolated so that there is no free access to the Institute's other facilities.

6.1.9 Access and protection in connection with tenants in the building

Tenancies at the Institute's domicile must be in separate buildings from the company areas and have their own locking/ key system.

It must be ensured that the tenants do not have equipment or machines that can disrupt operations at the domicile (electrical noise, noise, vibrations, other), and that no work is carried out with production or materials which can expose the building to physical risks such as fire, explosion etc.

When using joint LAN (physical or wireless) it is up to this individual party to protect access to own IT systems.

6.1.10 Security in connection with renovation

In cases of renovation and removals in IT areas or similar operationally sensitive areas, and where the area will be open to random access because of the building work,

special controls must be introduced to ensure that the company's security is not compromised and that assets are not exposed to unnecessary damage or theft.

6.1.11 Alarms, monitoring and inspection rounds

Particularly sensitive areas of the company must be protected with burglary alarms in all rooms with doors and windows at ground level, or alternatively follow the rules for room classification and zone division. Alarms must have direct call-up to the security center.

Inspection rounds must be carried out at specified fixed times. Calls to and attendance by the security center must be able to be documented (for insurance purposes).

6.2 IT equipment and other technological equipment, supply security

6.2.1 Location of IT and technology facilities in the building

Central and joint IT equipment as well as other vulnerable and operationally crucial equipment must be located in locked rooms dedicated to the purpose with special protection of the physical environment, e.g. in accordance with a zone division and room classification. The facilities must not be marked on generally accessible plans and must not be marked with direct signposting.

6.2.2 Requirements to location of IT equipment in technology facilities

The IT equipment must be placed on shelves and racks with room for operation and service from both sides as a minimum according to requirements from machine suppliers. All machines and cables must be marked with name, use, connection points and other relevant information.

6.2.3 Power supply and alarm in case of power problems

The IT equipment must be supplied from two separate entrance sources to the building, distributed to separate fuse groups with voltage equalizers.

Operationally crucial units must be protected against power cuts with UPS equipment. The capacity of the UPS must be determined on the basis of the operational consequence of a break-down. The UPS must be tested periodically.

The power supply must be monitored with alarm to IT or another manned location.

Needs for emergency diesel generator(s) must be assessed periodically on the basis of operational dependency and consequence of a power cut of long duration. Any other emergency power supply must be tested regularly.

6.2.4 Cooling and ventilation – alarm in case of failure

IT and technology facilities must be protected with sufficient and constant ventilation and cooling which lives up to the specifications of the IT suppliers.

There must be sensors which can alert the IT employees or others in case of a significant reduction or failure in the cooling systems. Ventilation channels must be provided with automatic fire dampers which are closed and operated by the fire alarm system.

The need for power protection of IT supply equipment (cooling, ventilation) must be assessed regularly. Needs for emergency diesel generator(s) must be assessed periodically on the basis of operational dependency and consequence of a power cut.

6.2.5 Protection against damp and water damage – alarm

Equipment must not be placed near or under continuous water pipes. Special attention must be paid around skylights to prevent leaks and water penetration. Equipment and cable joints must be raised at least 40 cm above floor level if there are continuous water pipes and/or drains in the floor (cellars).

If there are drains, then reflux valves must be installed. A damp alarm must be installed under the floor with direct call-up to the IT employees or other security staff. If it is relevant for the area, a ground water pump must be installed (cellars).

6.2.6 Fire prevention and alarm

Crucial IT and technology facilities must be provided with statutory fire fighting equipment and with sensors (smoke, heat or ion detectors) for automatic fire detection, alarm, (possibly with an Early Warning System) and with automatic release of extinguishing agent. No flammable materials may be stored in the facilities or in nearby facilities. Furthermore, smoking and use of direct fire is prohibited.

6.2.7 Protection of cables and crossfields

Cables must be protected against breakages and being torn out. The cables must be joined in cable trays and shafts. Data cables must, as far as possible, not be routed parallel in the same tray as electricity cables. Crossfields must be established in locked units with video monitoring. All IT cables must be marked with use, addresses or other relevant information.

All cable routings in walls and storey partitions must be blocked with fire resistant materials.

6.3 Acquisition, maintenance and discarding

6.3.1 Acquisition, approval procedures

Through its purchasing policy and contracts the company must ensure that IT equipment, IT supply and auxiliary equipment can live up to the intentions in this IT security policy with regard to operational stability, access protection, break-down frequency and time consumption for restoration after break-downs. The security requirements must be reflected in requirements to suppliers.

New IT equipment must be tested against the stated requirements and fully live up to the important points. The final purchase must be approved.

6.3.2 Service agreements, spare parts situation

Service agreements with coverage within the company's normal operating period should be made for units and systems which are especially crucial for operations.

Especially crucial spare parts must be in stock at all times with the supplier in Denmark, or alternatively the supplier must be able to deliver replacement equipment within the agreed deadlines.

6.3.3 Installation of hardware and software

Every installation of hardware and/or software must be planned, executed and tested systematically according to current Change Management procedures.

Setup of configuration and security parameters must, as a minimum, live up to this IT security policy.

6.3.4 Moving or removing equipment

IT equipment (with the exception of portable equipment) must not be removed from the company.

6.3.5 Sale of IT equipment

If IT equipment with built-in data storage is sold (disc or similar), then this must be overwritten or deleted securely with special program tools so that data cannot be restored with generally known techniques and tools. Deletion must be carried out and monitored internally before being handed over to a new owner. Sale of equipment must be approved.

7 SECURITY DURING OPERATION / PRODUCTION

7.1 Operational conditions, batch production

7.1.1 Operational planning

The IT operation must be planned in such a way that both daily and periodical operation can be executed correctly and punctually. The operational plan must be drawn up in good time in cooperation with relevant users.

7.1.2 Operational documentation

There must be actual operational documentation which describes the machine and system environment as well as the various operational tasks, manual and mechanic.

7.1.3 Execution of operations

The IT operation must be executed cf. the operational plan in such a way that both daily and periodical operation can be executed correctly and punctually. The operational plan and documentation must be available to the operator.

7.1.4 Operational window

Primary operational window: All working days between 7 a.m. and 6 p.m.

Secondary operational window: All working days between 6 p.m. and 12 midnights and all nonworking days between 7 a.m. and 12 midnight.

Service window: Every day between 12 midnight and 7 a.m.

All planned downtime must be announced at least 24 hours before.

Planned downtime may not take place in the primary operational window. Exceptions must be approved by the IT Manager.

7.1.5 Operational monitoring and inspection

The IT operation must be continuously monitored with a view to fast remedial action in case of problems, errors and delays. As far as possible, monitoring must be automatic. The operator must sign a receipt for executed manual inspections. Necessary monitoring must be established in connection with the execution of particularly crucial operations.

7.1.6 Operational reporting

All deviations from normal operations as well as every error which occurs (hardware, software, application, data and other) must be registered continuously and collected in periodic reports. Problems and errors involving operations and/or security must be

reported separately to the manager in charge and in accordance with specified agreement.

7.1.7 Supply and storage of commodities

The ongoing supply of commodities must be ensured via supplier contracts and checkpoints in the purchasing procedures. There must be contracts with more than one supplier for important commodities.

Various IT related commodities must be stored in special locked units to which only authorized personnel have access. Storage and use of particularly valuable materials and value forms must follow separately described rules and business procedures. These matters will be subject to periodical review.

7.1.8 Change Management

Updating and changes in any system may only be carried out by the Systems Manager, and changes must be executed as far as possible outside the primary operational window.

Backup persons with proper access to the system may only carry out updates and changes in the system after prior written agreement with the Systems Manager.

The Systems Manager can allocate time limited rights to systems to other people (consultants and developers) after written agreement and with approval from the IT Management.

In connection with any change in the Institute's systems which is classified as Priority 1 and 2, prior information must be submitted to the Change Management Box. All irregularities in systems, including restart of systems and services, must be reported here.

Planned changes which affect the employees' use of the systems must have prior approval from the IT Management.

All significant changes or irregularities which affect the employees' use of systems must be reported in the Driftsinfo (Operational Info). Reports in Driftsinfo must include scope and expected time of execution.

7.2 Specially for operations at external service suppliers

7.2.1 Definition of the delivery, incl. security aspects

When entering into operational agreements on outsourcing and/or housing, the required IT security level must be determined in the contract. The security level for the relevant areas must not be lower than the one described in this IT security policy. The supplier must be able to document that he can live up to both the content and the

intentions before entering into the agreement. Any deviations must be assessed and approved. A person to be in charge of communication, coordination and follow up of activities between the Institute and the supplier will be appointed.

7.2.2 Monitoring and review of service supplier

Demands will be made with regard to monitoring, inspection and review of the supplier's handling of tasks, including reporting errors and occurrences which might compromise the company's IT security. The supplier may be instructed to report immediately particular defined occurrences.

Reported occurrences will be collected and reviewed and specified status meetings with the supplier.

Upon request the supplier must be able to present an audit report without significant endorsements regarding the operational and security conditions to which the company attaches great importance.

7.3 Crucial components, classification and registration

7.3.1 Crucial hardware components

IT must be aware of which parts/units of the configuration can be crucial for operations.

7.3.2 Crucial software components

IT must be aware of which parts of the configuration – and which software components (basis systems, operative systems and the like) – can be crucial for operations.

7.3.3 Crucial program and data components

IT must be aware of which parts of the configuration – and which program and data components (business applications, data bases, registers) – can be crucial for operations.

7.3.4 Crucial license keys, passwords etc.

Program licenses (codes, system keys, other), password for crucial units, encryption keys, codes etc., must be stored securely and protected from physical damage and unauthorized access.

The IT operational staff must be able to have free access to the codes in connection with serious operational problems, critical situations and stand-by.

7.3.5 Crucial operations, alternate options – stand-by

IT must be aware of how operations can be continued and to what extent in various crisis situations.

7.4 Program application

7.4.1 Application of software in the company

The Institute must base its IT application on recognized standard programs, supplemented with programs developed by the Institute. IT must keep a list of approved programs (a positive list).

Requests for other programs must be submitted for approval.

7.4.2 Download and installation of software

The employees may only download and install programs on the Institute's workstations to a limited extent and only if these programs are necessary for the review of specific information or to perform daily tasks.

The IT department reserves the right at all times to deny the user access to the network if installed software is considered a security risk, or if it is in breach of licensing regulations.

Any requests for special programs must be submitted to the IT Manager. Assessment of the acquisition will take place together with the future system owner and must follow the policy for purchasing software and applications. The acquisition is subject to approval.

Only employees from IT service may download and install programs on the Institute's servers.

7.4.3 Protection against harmful programs

The Institute's IT systems must be protected against infiltration from harmful programs by setup of relevant hardware and software filters on servers, gateways, firewalls, work stations, mail systems etc.

The setup must be documented and followed in case of system changes and installations.

7.4.4 Protection against computer vira

All relevant IT units must be protected with anti virus software which must be updated on an ongoing basis. Portable IT equipment (computers and other) must be updated automatically by connection to the company's network. All loose data

carrying media must be monitored for virus before use, if possible automatically. All in and outgoing e-mails must be monitored automatically for vira.

All protected must be monitored (scanned) for vira at specific intervals.

7.4.5 Protection against adware and spyware

IT units with direct access to the Internet must be protected against intruding spyware. The anti spyware system must be updated regularly. Total spyware inspection must be carried out regularly on crucial IT units.

Traces of adware must be removed in the same or similar computer run.

Portable computers must be updated by connection to the company network.

7.4.6 Protection against spam – incoming

The Institute must protect its e-mail systems against incoming spam by setting up filters.

The filtration must be supported by subscribing to SPAM addresses. The filters must be kept fully updated. Portable computers must be updated by connection to the company network. There must be a procedure for clean-up after possible spam attacks.

7.4.7 Protection against spam – internally

Employees are not permitted to send SPAM mails such as jokes, chain letters and the like on the company network. A breach of these rules can have consequences for the employment relationship.

7.4.8 Protection against spam – outgoing

Unsolicited promotional messages may not be sent to the company's customer in the form of e-mails.

A breach of these rules may have consequences for the employment relationship.

8 PROTECTION OF THE INSTITUTE'S DATA

8.1 Physical data protection

8.1.1 Protection of system and configuration files

System technical data must be backed up before any large system changes or other risky activities are started.

The copies must be kept separated from the original data and be stored in a fireproof safe (or specific premises), classified minimum as S60DIS. The copies must at least

be placed on a different address or building or of equal distance. Alternatively, a remotely placed a backup service may be used.

8.1.2 Backup and safekeeping of data copies

Data belonging to the Institute must be backed up before any large system changes or other risky activities are started.

The copies must be kept separated from the original data and be stored in a fireproof safe (or specific premises), classified minimum as S60DIS. The copies must at least be placed on a different address or building or of equal distance. Alternatively, a remotely placed a backup service may be used.

8.1.3 Archiving of backups according to legislation

Accounting records must be archived according to the Bookkeeping act, in a form and a format that may be rendered in a readable format, or alternately be archived as paper. A copy of the accounting program and the corresponding database version must be kept together with the data in a fireproof environment related to the selected safekeeping.

8.1.4 Backup copies in the event of change of technology

The institute must secure that the continued access and readability of old data (backup copies), in connection with the internal shift of technology, according to the Institute's regulations for data classification. It must always be possible to transfer business critical files to the new technology by simply copying or converting them.

8.1.5 Utilization of backups from the data files

Backups may only be taken out from manual data files (fire safes, archive rooms, or other) for use in special instances, and only by staff with specific access privileges. Backups from remote backup must be copied – not moved. Removal and use of backups must be registered for control purposes.

Backups (physical) that are removed must be brought back promptly after use. By longer use, the media must be copied, and one of the copies must be returned to the data archive.

This copy must be deleted, by overwriting, immediately after use.

8.1.6 Control of backups in secure archive

Periodically there must be carried out a control, that the data media are present in the security archive (fireproof safe, archive room, other).

8.1.7 Security concerning the use of data carrying media

Transfer of confidential and private data to independent data carrying media (floppy disks, CDs, tapes, USBs, etc.), beyond backup copying, must only be used in specific situations, and must be approved.

8.1.8 Storage of business data

All information should be kept on the Institute's systems and networks. Transfer of company information to hard drives is only permitted in the form of copying, and should not include confidential or sensitive personal information.

In cases where material is prepared when not connected to the Institute's networks, the material should be copied to the Institute's systems and networks at the earliest opportunity.

8.1.9 Handling of discarded data carrying media

Data carrying media that are about to be discarded (USB, floppy disks, CDs) must be delivered to the IT department, who, in turn will delete or physically destroy the media.

8.2 Protection of data in connection with data transfer

8.2.1 Shipping and transport of data carrying media

Physical shipment of business information on data carrying media (floppy disks, CDs, tapes, USB, etc.) to partners, vendors or others, must only be done in agreement with the owner of the data, and if the data is business critical or sensitive personal information, the content must be encrypted.

Only encryption software approved by the IT department must be used for this purpose.

8.2.2 Electronic distribution of business information

Electronic transfer of business information (e-mail, file transfer or similar) to partners, vendors, or others should only be done in agreement with the data owner, and if the data are business critical or personal sensitive information, they must be encrypted. Only encryption software approved by the IT department must be used for this purpose.

8.2.3 Data security in regards to printing

Particular attention must be given in connection with printed content and who might be able to read it while printing.

8.2.4 Data security in connection with the use of fax-machines

Especial concern must be paid concerning information content, and who might have the possibilities to read the content in connection with fax exchanges.

8.2.5 Exchange of data with public authority

When exchanging data with the public authorities, specific attention must be paid to the quality of the data before transfer. Data may be exchanged after an agreement with the authority in question.

8.2.6 Security around transfer of data abroad

Transfer of data that are business critical or personal sensitive in content, to parties abroad (e-mail, files, backups, etc. either sent via communication lines or are transferred on physical media), must be limited.

8.2.7 The use of encryption

If there is a need for encryption of documents, e-mails and other material – please see the related issues in this IT security policy.

Only symmetrical encryption must be used, in addition to the Institute's authorized encryption program. Encryption codes are handed out by the "key" administration.

9 TO SECURE THE INSTITUTE'S NETWORK AND COMMUNICATION

9.1 Operational conditions, network operation

9.1.1 Network documentation

A technical network documentation, that is relevant, detailed and updated, must be available for the company's local network and external connections.

The documentation must be detailed enough for 3rd parties (e.g. consultants) may use them in an emergency situation.

9.1.2 Network monitoring and control

The network operation must be kept under constant control, locally or via remote monitoring, for speedy alleviating problems and errors. As far as possible, monitoring must be automatic. The use of remote monitoring requires approval of the utilized solution.

Automatic monitoring must be able so send alarms to the IT staff. Necessary monitoring shift arrangements must be established in connection with the execution of particularly crucial operations.

9.1.3 Reporting, network operation

Substantial network problems and errors must be registered.

9.1.4 Change Management, network

Changes in the network configuration, communication systems or equivalent, must be presented to the IT management to secure the co-existence with the present and ensure correct implementation. The change is the responsibility of the owner of the system, and it is carried through, if possible by several persons (functional separation).

9.1.5 Activity logging and error reports

A permanent logging of all traffic on the network will be carried out. Logging is done in three areas: Internal traffic, internal communication, and intern/dmz.

9.2 Securing the Institute's communication lines

9.2.1 Securing the Institute's communication lines

The Institute's electronic communication lines and systems must be secured in such a way that unauthorized intervention, listening in, wiretapping and other which may destroy, limit, manipulate or lead to misuse of the systems.

Securing of communication over open connections must be emphasized (Internet, wireless communication, mobile transmission, etc.) The security methods must be continuously checked, and new techniques must be evaluated.

9.2.2 Network topology and configuration

The internal network must be constructed as simple as possible, and be flexible enough to be expanded and changed as needed.

The network should be divided into zones, to minimize loss and compromising of the data. In addition it needs to be secured against that a break down in one place knocks down other parts.

The network component (hardware and software) must be from reputable producers and must be according to current standards concerning communication and security. If communication is done via public stretches between branches or departments, the communication must be secured against foreign intrusion.

9.2.3 Internet connection and the use of a firewall

Internet connection must only be accomplished from the Institute's computers and network.

The connection must be protected and zone divided with one or more firewalls.

The setup parameters of the firewall, as well as the rules for computers and firewall must be backed up and checked periodically, and always in connection with changes to the network (new programs or units).

The firewall must be tested periodically by external port scanning.

9.2.4 Filtering of incoming data stream through firewall

Generally used file formats, which are used in the Institute, must be led through. Packed and executable files must be filtered out; to the extent they represent a security risk. The receiver must be advised and approve the transfer to the local network.

Data from unwanted senders must be filtered away. The IT department will maintain these filters.

9.2.5 Filtering of the outgoing data stream through firewall

Generally used file formats, which are used in the Institute, must be led through. Packed and executable files must be filtered out; to the extent they represent a security risk. The sender must be advised and will have to give a reason for the transfer before it is executed.

If needed, file transfer from named users and/or workstations may be shut down. This blockage and the user's possible wishes to send files must be approved.

9.2.6 Dial-in / dial-out

The use of modem in workstations or similar, which at the same time are connected the institute's network, must only be done after the IT departments approval and must be based on specific system needs.

The modem must only be physically connected to the phone network when it is in use.

9.2.7 Safeguarding of ports for service and diagnosis

Service and diagnosis ports on IT equipment should usually be blocked, but may be used by approved partners for upgrade and service purposes after agreement with the IT responsible.

9.2.8 Use and safeguarding of wireless connections

The use of wireless connections in the Institute's networks must be protected against wiretapping, information snatching and against foreign penetration. Wireless equipment must only be connected to the Institute's local network through the Institutes firewall. Wireless equipment must only be used in agreement with IT.

9.2.9 Connection of network equipment

Only equipment approved by the IT department must be connected to the Institute's networks (Local network and Labnet). Connection of equipment, like laboratory equipment, must only be done with prior approval from IT.

Network connections, tokens for remote access, network equipment and all computer accounts to the network must be deactivated if they are not used for three months.

IT reserves the right, at any time – with no prior notice, to shut the systems down for security reasons. This concerns the local network, the Lab-net and the Guest net. System requirements concerning connection to these networks may be seen in the Network classification.

9.2.10 Safeguarding in concerning connection from remote workstations

Connecting to the Institute's network remotely (from home, hotels or other companies, hot-spots etc.) must only be done through special secure lines (e.g. VPN tunneling) and with 2-factor identification and validation. The remote equipment must, if possible, be secured with a firewall.

9.2.11 Data transfer via mobile phone

Connecting to the Institute's network from mobile phones must only be done using special secure lines (e.g. VPN tunneling) and with 2-factor identification and validation.

9.2.12 Security by the use of network analyzer

The use of a network analyzer, with external assistance, must be monitored by one of the Institute's IT employees. The scope of the task must be documented and approved of the responsible IT employee.

The collected data must not be removed from the Institute.

9.3 Operation of network or web sites located at external service vendor

9.3.1 Definition of the delivery, incl. security aspects

When entering operating agreements for networks, other communication equipment and web sites (housing), the required security level must be specifically determined in the contract with the description of physical framework and who should be able to access the Institute's equipment.

In agreements concerning outsourcing, the IT security must be determined based on the tasks the vendor will carry out, and specific points must be made regarding access to the Institute's systems, data, and backup routines.

9.3.2 Monitoring and review of service supplier

When entering service agreements for networks, other communication equipment and web sites with external vendors, the Institute must require monitoring, control and audit of the vendor's handling of the tasks, including reporting of errors and incidents which may compromise the IT security of the business.

The vendor must be able to present an audit report with no substantial comments concerning the conditions the company ranks highest.

10 ACCESS MANAGEMENT FOR SYSTEMS AND DATA

10.1 Administration of user access and privileges

10.1.1 Principal management of access to the IT systems

Access to the Institute's systems and data must be role based, and thus mirror the daily work. Access to the IT systems and data must be given on a need-to-know basis.

The roles are established in collaboration with the owners of systems and data, in addition to IT. The roles, which must be documented, are evaluated and adjusted as needed, e.g. in connection with organizational changes or similar change in the business.

Only employees who have been assigned initials, and have signed an agreement may access the Institute's networks.

Assignment of accesses to all central systems must be approved by HR and must be sent in writing to the User setup group.

10.1.2 Assignment of IT accesses and privileges

New employees are given access privileges to systems and data required to their job description (role). IT employees are assigned special user IDs (system accounts), for use with technical tasks.

Network access is assigned no later than the employees first work day. All assignments and changes are reported in writing to the User creation group. Access to common resources in the institute and local resources is given dependent on the work area.

The password will be given to the employee upon application to IT. The password must be reset and corrected at the first login.

10.1.3 The structure of passwords

The responsible manager must inform the HR department about hiring, changes and resignations.

The administration of the users of the systems must be carried out from a functional separation point of view.

All user administration must be reported to the User creation group for control and audit.

Personal password to the IT systems must be sufficiently complex within the frames the IT systems make available.

Passwords must be unique, and must not be reused, or be similar to others that have been used. The systems must, if possible, control these rules automatically.

10.1.4 Assigning commune user access

Common user identification and password must be assigned to a group of employees with specific tasks. The user profile (Lab accounts) must only be created by IT, and the account must not give access to personal resources, including mail.

10.1.5 Assigning of periodical privileges

In connection with replacements in vacations or similar, where one user (employee, temp or other) needs periodical access and privileges:

Employees may give colleagues access to their Outlook information through privilege handling. Substitute privileges in Outlook must not be used (send on behalf of), with the exception of resource mailboxes.

Automatic forwarding of e-mail should only be done to another mail address within the Institute, and never externally for the Institute.

Passwords to networks are private and should never be shared.

Other privilege assignments than the affected employee must be approved in writing of HR or the top management, and be sent in writing to User create.

10.1.6 Change in IT privileges with change of duty or department

As soon as an employee changes duty or department, his or her user access and privileges to the IT systems and data must be changed. The changes must be reported to HR. Control of access and privileges are to be sent in writing to User Create, and should be revised promptly.

10.1.7 Transfer of IT ownerships with change of duty or department

When an employee changes duties or departments, the supervisor must secure that ownerships are transferred to other employees, and that the data on the vacant computer (stationary and/or laptop) is transferred to the other employee as soon as possible.

Computers, mobile phones, and other data media must be handed in to IT for cleaning before they are passed on to another employee. Data carrying media which have belonged to managers must be destroyed by IT.

Automatic access to common resources in the institute and local resources is given dependent on the work area Phone number, e-mail address, mailbox and personal disks are kept unchanged to move with the employee.

10.1.8 Limitation of login attempts

If the individual access systems can be set up for it, incorrect login attempts should be limited automatically. After the maximum number of attempts has been reached, the user will either be blocked for an amount of time, or be permanently blocked and given a new password.

The reason for the incorrect login attempts must be investigated (error or intrusion trial), and the users who repeatedly have problems with the correct login must be supervised.

10.1.9 Password – resetting

If a user has forgotten the password, he or she must contact the system administrator in person, or via phone, who in turn can reset the user's password.

Passwords belonging to network accounts can only be reset after a check of the cell phone number or personal attendance (compare with employee search). The system administrator may not change a password based on an e-mail or similar electronic

request without making a control phone call to the user, or send the new password via e-mail.

The user must change the assigned password immediately to a personal password. It must be checked that the user changes the password.

10.1.10 Work stations, unmanned

Monitors on work stations (including laptops) must be "shut off" automatically after a defined (short) time frame without any activity, and when the work place is left for short period of time. The monitor is "started again" with a password or physically identification (card, token, biometry, other). The work station must be shut down when the workplace is left for a longer period of time, for instance at the end of the work day.

10.1.11 Audit and control of user accounts

To secure that the user accounts are current, a continuous control must be carried out. Inactivity for 3 months will result in blocking of:

Network accounts: Can be reopened by IT based on a check of the employment status.
VPN access: Can be reopened by IT based on a check of the employment status.
Network connection: Reopened by contacting IT
PC or other hardware: Reopening of access can only take place after the equipment has been updated.

If the employee does not receive salary for three months, the network accounts will also be automatically blocked.

The reasons must be investigated, and the user account deleted, if necessary. If the user has resigned, it must be checked that the ownerships, data, etc. has been transferred to others.

10.1.12 Audit and control of the users privileges

Owners of systems and data, or alternatively another named employee, should by set intervals revise the active user population, the user accesses and the rights to IT systems and data, in addition to carry out spot tests to check the continuous changes. Requisitions and factual privileges must be compared.

10.1.13 Physical safeguarding unmonitored IT equipment

Unmonitored IT equipment, placed in publicly accessible areas must be safeguarded against theft by labeling them.

10.1.14 Logical safeguarding unmonitored IT equipment

Software and any data in unmonitored IT equipment (e.g. PC based customer terminals), must be refreshed automatically by intervals with reasonable intervals based on the number of users, in addition to the informational value the terminal has for the customers.

10.1.15 Logging of user activities

Automatic logging of the activities in the systems must describe the users' behavior concerning accesses (to the network, programs and data), internet use, e-mail, etc. The users must be made aware that all information may be logged.

The log information must be treated confidential, and must only be used internally.

Direct monitoring of selected employees is carried out when it is assumed that noise, hacking and misuse is going on, after a written notification from HR or the top management.

All external e-mail (including all subjects in Outlook) is logged and filed. It is not possible to delete e-mails at the Danish Technological Institute.

All connections with remote devices – and attempts at connection – will be logged with information on the access taking user/pc as well as the point in time of connection and disconnection.

10.2 Management of network accessibility

10.2.1 Identification and authorization of the users

The access to the company's IT-network should primarily be secured with password. For places with special control is needed, there should be used a 2 factor identification.

10.2.2 Identification of employed network equipment

The access control for connection of portable equipment to the company's network may be supplemented with identification of the hardware identity.

10.3.6 Management of periods of usage, automatic interruption

Access to the company's IT network, may be limited to regular work hours + a number of hours before and after. The IT management must approve any extraordinary access. Access must be limited in time for non employees: Consultants, developers and similar external persons. The access period and access time from customer terminals and automats must be limited, where applicable.

10.3 Management of accessibility to operating systems and similar systems

10.3.1 Standard password for machines and systems

Standard passwords that come with new machines or systems must be changed when the machine or system is installed in the network. The password must be sufficiently complex and differ substantially from regular user passwords. It must be changed frequently, and specifically after the use of an emergency password or after and IT employee has resigned.

Passwords given to a technician or a consultant in connection with an installation or problem solving must be changed promptly after the word has ended. If the same password is used in several systems, the password must be changed simultaneously in all systems.

10.3.2 Use and control of emergency passwords

Logon information (user name and password) for access to critical units and systems must be written down, put in a sealed envelope and locked away in a fireproof locker.

The envelope may be opened in emergency situations, after (via phone) approval, when a key employee is not to be reached and the time is limited.

If the envelope has been opened, the used password must be changed immediately after the problems have been solved, and the envelope must be reestablished with a new password. The incident must be registered and reported.

10.3.3 Use of system tools

Use of system tools, which are able to by-pass the regular access, control, and security systems, should be used only by the IT employees with the necessary skills or education. The use must be approved before the work is started. The system tools must be secured against incidental and unlawful use.

10.3.4 Identification and authentication of users (basic systems)

Access to the company's IT basic systems (hardware, operating systems, etc) should only be given to the employees in the IT department, and be secured with password. Access to especially sensitive systems should be secured with a 2 factor control.

10.3.5 Identification and authentication of users (business systems)

The access to the company's IT business systems must primarily be secured with password. For places with special control is needed, there should be used a 2 factor identification.

10.3.6 Management of user periods, automatic interruption

Access to the company's IT business systems and data, may be limited to regular work hours + a number of hours before and after. Access must be limited in time for non employees:

Consultants, developers and similar external. The access period and access time from customer terminals and automats must be limited, where applicable.

11 SYSTEM AND PROGRAM DEVELOPMENT, – MAINTENANCE ETC.

11.1 Standard applications

11.1.1 Procurement and evaluation – applications

All procurement of applications must be channeled through the IT department, who will evaluate the relevance of the product, collaboration with other systems, security, etc. The desired software and applications must be tested and evaluated before it is implemented in the production environment. The procurement must be approved of the future system owner.

11.1.2 Licensing and control

The business must comply with current legislation in the area, in addition to the vendors specific license agreements. The IT department must register all purchased software / applications with notes concerning the number of purchased licenses. The actual number of licenses in use must be controlled at least once a year, and always in connection with renewal of licenses.

11.1.3 Test, approval and start-up

All software and corrections/upgrades must be tested before implementation in the operational environment.

Implementation should only be done with approval from the IT operating management.

11.1.4 Maintenance, upgrade

Standard software must be updated frequently, as often as the vendor is releasing updates/corrections, and in a way that ensures compatibility with other systems. The relevance of any corrections must be evaluated, the corrections prioritized and the installation must be in accordance with the requirements for testing.

Updating of PC is distributed centrally. Antivirus software should have a local update profile towards the antivirus supplier, which fetches updated directly within 3 hours of login.

The system owner is responsible for security updates of the machines on the Special network and the Guest network.

Updates of the servers are taken care of manually in the Operating department. Updates are done every month, Wednesday evenings between 9 PM and 12 PM. Critical updates are installed as fast as possible after approval from the IT management. All installed updates must be thoroughly tested by the system responsible before any changes are done and a green light is sent to the person responsible for operation.

11.2 Development of applications in general

11.2.1 Definition of the development task, incl. security aspects

A description of the task and a sufficient specification of the requirements must be in place for any development project.

Special focus must be paid to the security concerning the data handling, built in controls for data validation, calculations, data exchange, etc. for the systems, in addition to management and control of user access and privileges. It is necessary to discuss and implement all security aspects, including risks and evaluation of consequences.

11.2.2 Security aspects regarding the system

In connection with design and development of new systems, all security aspects and influences of existing systems, electronic procedures and manual business routines must be specified and evaluated.

An analysis of the consequences for the business if the system is down, must be prepared. An approval must be available, stating that the application is according to requirements and intentions in the current security policy.

11.2.3 Definition of the system's built-in controls

The built-in controls in the system must be documented. Necessary external controls of input/output data must be documented.

11.2.4. Access control and user management in new applications

Necessary control of user access to the system, the features and data must be managed on a role basis, including administration of the access privileges in all new

application development. Un-authorized programs must be prevented accessing the data accordingly. The passwords in use must be stored and secured in encrypted format. Access to essential functions and sensitive data must be logged, and made available for audit.

11.2.5 Development and safeguarding of system documentation

Necessary system documentation must be developed from the start of the project.

The system documentation, including diagrams, drawings, tables, etc. must be filed.

11.2.6 Rights and copyright to design and code

The business is the sole owner of all rights to the applications developed of employees, and this must be a part of the employees' employment contract.

The business' copyright, user right and the rights to change the applications must be agreed upon, and be a part of the contract with an external developer. It must be possible to make necessary corrections without the primary developer, if this is not available or has the possibility to make the corrections within the company's time limit and needs.

11.2.7 Version management and edition management of program editions

Developers – both internal and external – must utilize version management in the development progress.

11.2.8 Use of production data for test purposes

Only copies of production data should be used for testing purposes, after this is approved by the responsible owner of the system and data. Business critical data and data covered by the legislation concerning databases should only be used to a limited extent, and must be made anonymous before they are used. Use of this kind of data must be substantiated in writing.

Such data must be secured and kept according to the same security and safety requirements as stated in the current IT security policy. Any transfer to external developers can only be done after approval from the data owner.

11.2.9 Test, approval and start-up of business systems

All business systems, new, corrections and upgrades of such, must be tested before they are implemented in the operating environment. Implementation should only be done with approval from the IT operating management.

11.3 Specifics for externally developed programs

11.3.1 Source code deposit for externally developed programs

Especially critical systems must be secured by depositing a copy of the program code, – all versions – in addition to a copy of relevant documentation to secure access to the code and further development. This requirement must be noted in all development contracts. The deposit must be documented continuously.

Access to the code must be possible within 30 days from a possible bankruptcy of the developing company.

11.3.2 The vendors access to production data in test situations

Only copies of production data should be used for testing purposes, after this is approved by the responsible owner of the system and data. Business critical data and data covered by the legislation concerning databases should only be used to a limited extent, and must be made anonymous before they are used. Use of this kind of data must be substantiated in writing. The reasoning should be filed for audit purposes.

The vendor must delete all test data, including any backups immediately after approval of the test results.

11.4 Administration and management of web sites.

11.4.1 Management and control of the business' domain names

The IT department has the responsibility for the domain names, and they should keep an updated list over registered domain names. The list must be revised at least once a year.

Periodical controls must be carried out to check if other business have register .dk domain names that might lead to confusion among internet users. Cases that raise suspicion must be reported to DK-Hostmaster A/S (responsible body for all Danish domain names).

11.4.2 Responsibility for information maintenance on web sites

The content of the business' homepages must be kept current at all times. Homepages and CMS system (Content Management System) should have a responsible system and data owner. Access to create, content, change, edit and deletion of information is a part of the organization's regulations for (role based) access. The maintenance should be functionally separated with contributors and an editor, if possible.

11.4.3 Responsibilities for regulations and legislature concerning e-trade via websites

Content and descriptions on the company's homepages must as a minimum, be according to the legal demands for the area.

The descriptions should appear crisp and clear in layout and language, and be easy to navigate via menus, tabs or similar design technique. The texts must be controlled frequently and be adjusted according to any changes in the legislature.

The e-trade system should, if possible, be registered and approved with the e-mark of the E-trade fund.

11.4.4 Access to information via websites for customers and public

Access to the company's information systems should be ensured through precise identification of the user (customer/person), and the access to data should be limited to include the company's general information. The user identification and any password should be sent the customer in advance.

If the user will have access to his registered data, the access must be secured with a unique password, which must be sent to the user's mail or e-mail address in advance.

11.4.5 Tracking of customers' behavior on the homepage

User behavior must only be tracked from the company's homepages for statistical purposes. If the tracking is done on an IP address level, an advance user consent must have been received.

The users should always be informed about the tracking activities on the pages. The Registration Acts demands regarding collecting and storing of information must be observed.

12 MANAGING SECURITY ENQUIRIES

12.1 Warning systems

12.1.1 Advance warnings regarding coming security threats

The organization must subscribe to services which continuously and promptly warn about threats towards the IT security via e-mail and/or SMS to counter the threats.

There must be defense systems in place, and procedures for use to counter the threats, in addition to rectify the damages, if the defense is not sufficient.

12.2 Reporting

12.2.1 Reporting of security incidents

Security incidents are to be reported to the IT manager, and must promptly be registered. Found security breaches must be rectified promptly. An overview of security breaches must be presented at the first possible meeting in the IT council and/or be presented for the management.

12.2.2 Report of security weaknesses and exposures

Security weaknesses and found breaches must be reported to the IT manager immediately. The IT manager must continuously ensure that found security weaknesses and breaches must be rectified as soon as possible. A summary of security weaknesses and breaches must be presented in the first meeting in the IT council or be presented to the management in other ways for orientation.

12.2.3 Suspected – and found breaches of security

Ved mistanke om eller konstatering af brud på sikkerheden skal IT-chefen, alternativt nærmeste leder, informeres. Rapportering af hændelsen følger politik og regler for sikkerhedshændelser. Sikring af systemdokumentation og udbedring skal iværksættes omgående.

12.2.4. The use of log files for investigation

Alle systemlog´s skal sikres mod manipulation og sletning. Væsentlige system log's skal gemmes i en længere defineret periode. Log´s som beskriver brugeradfærd må kun kunne læses af IT-medarbejdere, og kun i forbindelse med løsning af aktuelle fejl eller kriminel investigering.

Adgang, databeskyttelse, sikkerhedskopiering med videre skal håndteres fortroligt.

12.3 Insurance and liability

12.3.1 Insurance

Virksomhedens forsikringer for IT området skal periodisk gennemgås med henblik på justeringer.

12.3.2 Ansvar ved brug af vagtselskaber

Virksomheden skal følge op på, at de aftalte vagt-/vægterydelser leveres tilfredsstillende.

12.4 Criminal acts

12.4.1 Handling criminal acts (staff)

Management must be immediately informed in the case of suspicion of criminal acts, or if a criminal act has been carried out that is harmful for the business, caused by staff, permanent or temporary, committing theft of equipment, software, etc., theft or misuse of business information, or manipulation of financial data. The management decides further actions in the business, and if the case should be reported to the police.

12.4.2 Handling criminal acts (external)

Management must be immediately informed in the case of suspicion of criminal acts, or if a criminal act has been carried out that is harmful for the business, caused by guests, vendors or others from the outside, committing theft of equipment, software, etc., theft or misuse of business information, or manipulation of financial data. The management decides further actions, and if the case should be reported to the police.

12.4.3 Securing and collecting evidence

When criminal actions towards the organization's IT systems are suspected or are found, it is vital that the necessary evidence is secured as soon as possible for possible use by the police authorities. Analysis of data holding media must, if possible, be carried out on copies.

12.4.4. The use of log files for investigation

Collected log files are immediately made available to investigate both problems and errors, e.g. in connection with investigation of the possibilities for, or a carried through criminal act.

Only the IT staff and possible called in IT specialists (including the police authorities) must be given access to the log files. Investigations must always be carried out on a copy of a given log file.

12.5 Controls and audit

12.5.1 General execution of controls

The management is responsible for having security regulations in place, and to make sure they are followed.

12.5.2 Internal IT audit

Through an internal IT audit, the company must ensure that the required security level is maintained, and that negative deviations are registered and improved.

13 RISK EVALUATION, VULNERABILITY AND CONSEQUENCES

13.1 Business risks and consequences

13.1.1 Evaluation of business risks

Consecutive analysis of Teknologisk Institut's most business critical systems must be carried out, i.e. the systems which are most costly, directly or indirectly, for the business when they are down (bottom line, liquid assets, customer loyalty).

The financial consequences of any substantial downtime for all of the business systems must be clarified. If the losses are accumulated, are the losses constant, is the system more sensitive in particular times of the month, certain week days or dates, etc.

Based on the estimated financial consequences, an overview of the most business critical systems must be prepared.

The IT infrastructure in the company is an absolute necessity for the operation of the other systems, and will therefore be a part of the analysis. If the IT infrastructure is down, it will normally not be a loss in itself, but rather represent a loss for the individual business systems.

In principle all systems must be classified according to the following model:

Primary systems P1
Secondary systems P2
Systems with no priority assignment P3

Inventories and procedures must be maintained for all P1 and P2 systems.

IT staff must have the necessary competence to operate the systems. In addition, consultants may be hired to advice and assist when system problems occur. A system administrator and a system backup must be pointed out for every system. The systems must be monitored at all times, and all data and system files must be backed up on a frequent basis.

Downtime for P1 systems is estimated to represent a commercial risk with more than 4 hours in the primary operating window and with more than 8 operating hours in the secondary operating window. And finally a downtime more than 10 workdays might represent a risk for the business.

Downtime for P2 systems is defined as being a risk for the business, if it lasts more than 8 hours in the primary operational window and more than 16 hours in the secondary operational window. And finally a downtime more than 15 workdays might represent a risk for the business.

Getting P1 systems back online must always have the highest priority. The organization must be oriented about alternatives and possibilities on a continuous basis, which will enable the staff to carry out their work.

13.1.2 Causes/probability for errors

In order to be able to counter and minimize substantial risks both with measures that are preventive and improving, constant identifying analysis must be carried out.

The systems must be evaluated with the intention to find the probability that they are struck with various incidents, both from internal and external sources, – e.g. erroneous use, technical errors on systems or machines, the probability for hacking and virus attack, power outages, internet failure, water damages, fire and other relevant causes. The occurrences might originate from within the organization; e.g. user errors, or lack of backups, or indirectly; e.g. a fire and chemical discharges from nearby businesses.

The analysis should at least be done on a yearly basis, or in connection with major IT-adjustments. New systems must be incorporated on a continuous basis in the existing analysis.

13.1.3 Critical components

Critical components must be identified on a continuous basis (e.g. servers, network points, databases, etc.) concerning a distribution of the risk where several business critical systems are hit at the same time by the same event, or by a domino effect.

Possible concurrence in utilization of hardware and system resources must be clarified, e.g. if databases and other files are placed on the same server, or if others common resources are utilized. A subsequent distribution of the business critical system to dedicated resources, in addition to limiting the consequences of an error, will often simplify emergency procedures and preparedness.

The Dataflow between the business critical system (critical data) must be identified with reference to specific security and control to reduce the possible consequences of data errors and shortages.

The analysis should be done on a yearly basis, or in connection with major IT-adjustments. New systems must be incorporated on a continuous basis in the existing analysis.

13.1.4 Uniform and simple

Systems and networks must be evaluated on a continuous basis, so that they are built as uniformly and simple as possible.

The objective is to use hardware and systems that are as common and thoroughly tested as possible.

As few hardware variations as possible should be used, and they should, if possible, be set up with the same configurations and settings. For that reason, the number of different vendors should be minimized.

Present IT competence must be taken into consideration when any new technology is introduced, and the evaluation of the competence must have a predominant influence when selecting technology, as long as it does not limit the development of the business in any considerable way.

13.1.5 Capability to change

The implementation and development of staff- or customer oriented systems must be evaluated regarding functionality and needs on a continuous basis.

Any system must be thought of as a set of functions and services, improving the business or reducing the costs.

Any bindings between functions or services must be minimized, both short and long term. When it comes to financial analysis, it must be considered that such bindings prevents future ability to change regarding the business, change in customer needs, changes in the organization, or changes in workflow. The analysis must take into account the additional costs this might lead to concerning development and implementation.

Systems for certain functions or services should be utilized as planned, and changes in data models should be avoided.

Concerning this, software development and implementation should be considered based on the same technical paradigm.