REGULATIONS ON USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

Laid down by the Financial Supervisory Authority of Norway on 21 May 2003 in pursuance of Act of 7 December 1956 No. 1 on Supervision of Credit Institutions, Insurance Companies and Securities Trading etc., (Financial Supervision Act) section 4 subsection 2, Act of 17 November 2000 No. 80 on Stock Exchange Activities section 3-4 first paragraph second sentence and Act of 17 December 1999 No. 95 on Payments Systems section 3-3 first paragraph second sentence.

Section 1 Scope of application

These regulations apply to Norwegian:

1. Commercial banks
2. Savings banks
3. Finance companies and mortgage companies
4. Insurance companies
5. Private, municipal and county municipal pension funds
6. Stock exchanges and authorised market places
7. Investment firms
8. Management companies for securities funds
9. Clearing houses
10. Securities registers
11. Debt collection agencies
12. Real estate agencies
13. Payment Institutions
14. E-money enterprises
15. Systems for payment services

These regulations apply to ICT systems of importance to the institution’s business. With regard to external users of the institution's ICT systems, agreements shall exist that ensure compliance with the regulations' requirements concerning security and documentation.

Section 2 Planning and organisation

The institution shall establish overarching objectives, strategies and security requirements for its ICT activity. It shall prepare a description of each process, and describe how responsibility for administration, procurement, development, operation, system maintenance, protection of data and discontinuation is to be discharged in a satisfactory manner.

The institution shall have guidelines that ensure that ICT activities that are outsourced comply with the requirements in Section 12.

The institution shall have designated persons responsible for the various parts of the ICT activity. The term 'designated person' means a function or position.

Outsourcing contracts and changes to such contracts shall be approved by the Board of Directors. The Board of Directors shall be presented with plans regarding the outsourcing, including risk assessments and a description of how the institution intends to control the outsourced ICT activities.

Section 3 Risk analysis

The institution shall establish criteria for acceptable risk in connection with its use of ICT systems.

The institution shall have a documented process for performing risk analyses of its ICT activities. The process shall clearly define responsibilities and it shall include follow-up measures to be taken as a result of the risk analyses.

At least annually, and in case of changes which influence its ICT security, the institution shall perform risk analyses to ensure that risk is managed within acceptable limits relative to the institution's business. The result of the risk analyses shall be documented.

Section 4 Quality

The institution shall establish quality objectives for its ICT activities that are consistent with the institution's overall objectives. The institution shall have in place documented procedures for monitoring compliance with established quality objectives.

Section 5 Security

The institution shall prepare procedures for ensuring that equipment, systems and information of significance for the institution's business, see section 1, are protected against damage, misuse, unauthorised access and change, and vandalism. The procedures shall also contain guidelines for the granting, modification, revocation and control of access to the ICT systems. As far as is practicable, security requirements shall be quantifiable. Fulfilment of the requirements for protection of personal data under Regulations of 15 December 2000 No. 1265 to the Personal Data Act shall be regarded as fulfilment of the requirements of this section.

Section 6 Development and procurement

The institution shall have written procedures for procurement, development, maintenance and testing of its ICT systems. The ICT systems shall not be put into operation until authorisation to do so is given.

Section 7 System maintenance

The institution shall ensure that its ICT systems are maintained and managed in a way that ensures stable, planned and predictable operation. There shall be documented procedures for system maintenance.

Section 8 Operation

Operation of the ICT shall be based on written procedures that ensure complete, timely and correct data processing and data storage.

The ICT operation, which shall be documented, shall ensure that ICT systems are available as specified in written requirements. To avoid disruption in the ICT systems or their environment that may negatively influence the written requirements, regular analyses and corresponding measures shall be implemented.

The institution shall test and document that the ICT operation is in line with the written requirements.

Section 9 Problem and change management

The institution shall ensure that procedures for the management of problems and changes exist and are complied with.

The procedures for problem management shall cover all problems that arise in the operation of the ICT systems. The objective of problem management is to restore normal operational conditions for the ICT activity. Problem management shall identify the cause of the problem as well as prevent its recurrence and shall ensure proper and formal treatment of the problem. The problems shall be documented. The procedures for problem management shall contain escalation guidelines.

Incidents that lead to a material reduction in functionality as a result of breach of confidentiality (data protection), integrity (protection against unauthorised changes) or availability of ICT systems and/or data, shall be reported to the Financial Supervisory Authority of Norway. Reporting shall normally cover events that the institution itself categorises as very serious or critical, but may also cover incidents that reveal vulnerabilities in applications, architecture, infrastructure or defence mechanisms. Institutions listed in section 1 first subsection no. 12 (real estate agencies) are exempt from the reporting requirement.

The change management procedures shall cover all changes that may affect the ICT systems and shall ensure proper, formal treatment and documentation of the changes. The institution shall ensure that the change management procedures provide stable, planned and predictable ICT operation.

Section 10 (Revoked)

Section 11 Disruption of operations and contingency management

The institution shall have a documented contingency plan which shall be activated if ICT operations cannot be upheld due to a contingency. The term 'contingency' means unintended events which cause a disruption such that the institution’s ICT operation is unable to continue with the regular set of resources.

The contingency plan must as a minimum include

- an overview of ICT systems included in the contingency plan
- a description of the contingency solution
- clear-cut criteria for activation of the contingency solution
- the acceptable downtime in case of disruption of operations before the contingency solution is activated
- procedures containing the actions necessary to restore the ICT operation
- an overview of responsibilities and procedures upon activation of the contingency solution
- directions for informing affected employees, suppliers, customers, public authorities and media.

Training, exercises and tests shall be conducted, at least once a year, on a scale that provides assurance that the contingency solution functions as intended. The results shall be documented.

Section 12 Outsourcing

The institution is responsible for ensuring that its ICT activity complies with all requirements imposed by these regulations. This responsibility also applies where all or parts of the ICT activity are outsourced. The supplier shall be contractually committed to supplying services that are consistently compliant with the ICT regulation. The agreement must ensure that the institution under supervision is given the right to control and audit activities carried out by the service provider under the agreement. The agreement shall also provide for secure management of confidential information.

The agreement shall further ensure that the Financial Supervisory Authority of Norway has access to information from the service provider and has a right to inspect the service provider, if the Financial Supervisory Authority of Norway deems this to be necessary as part of its supervision of the institution.

The institution shall, either directly or through formal collaboration with parties other than the service provider, ensure that it possesses sufficient competence to manage the outsourcing agreements.

Section 13 Documentation

A complete up-to-date overview shall exist of the organisation, equipment, ICT systems and significant factors related to ICT activities. Up-to-date documentation shall exist of each ICT system that supports the business, verifying compliance with the requirements of these regulations.

Section 14 Dispensation

The Financial Supervisory Authority of Norway may grant dispensation from these regulations or parts of them.

Section 15 Commencement

These regulations come into force on 1 August 2003. Regulations of 16 December 1992 No. 1157 on the use of information technology will be simultaneously revoked. The Financial Supervisory Authority of Norway may allow an institution to postpone compliance with requirements of these regulations.