

## **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 No. 1 of 7 December 1956 on Supervision of Credit Institutions, Insurance Companies and Securities Trading etc., (Financial Supervision Act) section 4 subsection 2, Act No. 80 of 17 November 2000 on Stock Exchange Activities section 3-4 first paragraph second sentence and Act No. 95 of 17 December 1999 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 E-money enterprises
14. Systems for payments services

The regulations embrace ICT systems of importance to the institution's business. To external users of the institutions ICT systems there shall exist agreements that ensure compliance with requirements concerning security and documentation of this regulation.

### **Section 2. Planning and organisation**

The institution shall establish overarching objectives and strategies for its ICT activity. It shall prepare a description of the individual processes and of how responsibility for administration, procurement, development, operation, systems maintenance, protection of data and decommissioning (of hardware) is organised with reference to recognised principles in the field.

When outsourcing the whole or part of the ICT activities the institution shall have separate guidelines specifically designed to ensure deliveries.

A party with in-house responsibility for the various aspects of the institution's ICT activity shall be designated. "Party with in-house responsibility" means a function or position.

### **Section 3. Risk analysis**

The institution shall establish criteria defining acceptable risk regarding its use of ICT systems.

The institution shall have a documented process for conducting risk analyses of its ICT activities. This process must define responsibilities and include monitoring actions/controls carried out as a result of the accomplished risk analysis.

The institution shall annually or more often if modifications of importance to the ICT security, conduct risk analyses to ensure that risk is contained within acceptable limits in relation to the institution's activity. The results of the risk analysis shall be documented.

### **Section 4. Quality objectives**

The institution shall establish quality objectives for each individual aspect of its ICT activity, and such quality objectives shall be consistent with the institution's overall objectives. The institution shall have documented follow-up routines ensuring compliance with established quality objectives.

### **Section 5. Security**

The institution shall prepare procedures designed to ensure protection of equipment, systems and data against damage, misuse, unauthorised access and vandalism. The procedures shall contain guidelines for allocation, change, deletion and control of authorisation to access the ICT systems. Security requirements shall as far as possible be measurable. Compliance with demands on security for processing of personal data according to Regulation No.1265 of 15 December 2000 on Personal Data Regulations, shall be regarded as compliant with the demands of this section.

### **Section 6. Development and procurement**

The institution shall have written routines for procurement, development, further development and testing of ICT systems. The ICT systems shall not be put into ordinary operation before the party with in-house responsibility has given its approval.

### **Section 7. System maintenance**

The institution shall ensure that its ICT systems are maintained and managed in a manner which provides a stable, planned and predictable operational situation. Separate guidelines shall exist which embrace all aspects of systems maintenance in keeping with recognised principles in the field. Documented procedures for system maintenance shall be available.

## **Section 8. Operations**

ICT operations shall be based on written procedures which ensure complete, timely and correct data production, handling and storage of production data and accessibility to the ICT systems.

## **Section 9. Problem and change management**

The institution shall ensure that procedures for managing problems and changes exist and are complied with.

The procedures for problem management shall embrace all problems which arise in the production systems. The object of the problem management is to re-establish normal operational conditions for the ICT activities. The problem management shall identify what caused the problem, as well as prevent recurrence and ensure proper and formal handling of the deviation. The problems shall be documented. The procedures for problem management shall contain escalation guidelines.

All deviations that lead to a material reduction in functionality caused by breach of confidentiality (data protection), integrity (protection against unauthorized changes) or availability of ICT-systems and/or data, shall be reported to the Financial Supervisory Authority of Norway. Normally, reporting applies to incidents considered very serious or critical by the institution, but should also encompass incidents that reveal vulnerabilities in applications, architecture, infrastructure or defence mechanisms. Institutions listed in §1 section 1 no. 5 (Private, municipal and county municipal pension funds), no. 11 (Debt collection agencies) and no. 12 (Real estate agencies) are exempt from the reporting duty.

The procedures for change management shall embrace all changes which may affect the production systems and shall ensure proper, formal handling and documentation of all changes. The institution must ensure that the procedures for change management provide stable, planned and predictable ICT operation.

## **Section 10. Continuity requirements**

The institution shall have an updated continuity plan. The institution shall establish a continuity procedure in which roles, responsibilities and risk are defined. With reference to risk analyse cf. section 3, the institution must identify ICT systems of importance to the institution which shall be included in the continuity plan. The continuity plan shall be a document which shall contain

- identification and assessment of risk components and actions to be initiated
- defined criteria for activating the backup solution
- recovery procedures
- directions for informing management, employees, customers and suppliers

Training, exercises and tests of back-up solutions shall be conducted to an extent which instils confidence that such solutions work satisfactorily. The tests shall be documented to enable their implementation and results to be assessed for the future.

### **Section 11 Disruption of operations and disaster preparedness**

The institution shall have a documented emergency plan which shall be activated if ICT operations cannot be maintained due to a disaster. "Disaster" means events which cause a disruption such that the institution's ICT operations are unable to continue using normally accessible resources.

The plan shall at minimum cover

- an overview of ICT systems included in the emergency plan
- a description of the disaster recovery solution
- defined criteria for activation of the disaster recovery solution
- acceptable time period for a disruption of operations before the disaster recovery solution is activated
- procedures containing the necessary actions to recover the ICT operations
- an overview of responsibilities and procedures at the activation of the disaster recovery solution
- directions for informing affected employees, suppliers, customers, public authorities and media.

Training, exercises and tests shall be conducted, at minimum once a year, and on a scale that instils sufficient confidence that the disaster response solution works 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. A written agreement providing this shall exist. The agreement must ensure that the institution under supervision is given a right to inspect and control activities carried out by the service provider according to 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 and has a right to supervise the service provider

if the Financial Supervisory Authority of Norway deems this be necessary as part of its supervision of the institution.

The institution shall, under its own auspices or through formalised collaboration with parties other than the service provider, ensure that its organisation possesses sufficient competence to manage outsourcing agreements.

### **Section 13. Documentation**

An assembled up-to-date overview shall exist of the organisation, equipment, systems and significant factors related to ICT activities. An up-to-date documentation shall exist of each ICT system important to the institution which document the compliance with the demands in this regulation.

### **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 No. 1157 of 16 December 1992 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.