Spillemyndigheden's Certification Programme

Information Security Management System

SCP.03.00.EN.2.0

Table of contents

1 Objectives of the Information Security Management System

The Information security management system shall ensure the protection of the gambling system and business systems against threats and secure sensitive information stored in the systems. Furthermore, a number of significant safety issues are safeguarded by ensuring the integrity of and access to the gambling system and business systems. Through the protection of sensitive information, concerns regarding confidentiality are met not only with regards to the license holder, but also with regards to players and third parties.

1.1 Scope of this document

This document contains the requirements specifying how testing organisations obtain accreditation for conducting certification of the gambling system, business processes and business systems of the licence holder as well as instructions on how to conduct the certification. The requirements concerning accreditation of the testing organisation and certification of the licence holder can be found in section 2 "Frequency and testing organisations".

To ensure the information security of the licence holder a number of requirements in relation to human resource management, communication and operation management, access control and the future development of the gambling system and the business systems must be observed. These requirements are set out in section 3 "Requirements for the information security management system".

1.2 Version

The Danish Gambling Authority continuously revises the certification programme. The latest version and the version history are accessible at The Danish Gambling Authority's website.

Date	Version	Description
2014.07.04	1.0	A new document structure than the previous version 1.3 alongside with a range of updates in different areas. A new version 1.0 is therefore published. It is the intention to follow normal versioning for future changes.
2015.12.21	1.1	Extension of applicability to cover offering of lotteries and betting on horse- and dog races.
2020.01.01	1.2	Spillemyndigheden has removed the requirement saying the ATO's accreditation must refer to a specific version cf. section 2.3.
2023.01.01	2.0	

When a new version of the certification programme is released, The Danish Gambling Authority will, if necessary, publish guidelines for a transition period and validity of already completed certifications.

It must be emphasised that only the Danish version is legally binding. The English version holds the status of guidance only.

1.3 Applicability

Information security management system is applicable for offering of:

- Online betting
- Land-based betting

- Online casino
- Lotteries

2 Frequency and testing organisations

2.1 Certification frequency

The licence holder is responsible to ensure to be certified in accordance with the requirements in this document with an interval of maximum of 12 months.

2.1.1 Initial certification

The licence holder must be certified before a licence to offer games can be issued, unless The Danish Gambling Authority has informed otherwise. See section 2.1.3 in the general requirements for further information.

2.1.2 Renewed certification

The licence holder must, as a rule, have completed a new certification within 12 months of the latest certification. The standard report must reflect, when the certification has been renewed.

The standard report, which documents the renewed certification, must be in the Danish Gambling Authority's possession no later than two months after the certification was done.

A renewal of the certification may be based on sampling, spot checks and compliance with the requirements set out in the document "SCP06.00.DK - Change Management Programme".

2.1.3 Postponement of renewed certification

The licence holder can choose to postpone the certification up to two months from the time where a new certification should have been completed. The new certification must be finalised no later than 14 months after the latest certification and the standard report must be submitted to The Danish Gambling Authority within the same deadline.

The Danish Gambling Authority must be notified before the certification is postponed.

The deadline for renewal of certification is shortened with the equally amount of time the former 12-month deadline has been postponed. Meaning that if you for instance make use of the maximum two months postponement, then the next certification is due 10 months later. The time for the next certification shall be reflected in the standard report.

The option to postpone the certification only applies to the licence holder. This means that the option does not apply to any suppliers the licence holder may have.

2.2 Accreditation in accordance with valid ISO/IEC 27001

If the licence holder is certified in accordance with a valid ISO/IEC 27001 it is to be expected that the information security management system of the licence holder is of such quality that it renders certification in accordance with The Danish Gambling Authority´s Information security management system SCP.03.00 unnecessary.

It is a precondition that certification of the information security management system is conducted as an accredited certification by a certification body, who is accredited after ISO/IEC 17021-1 for certification referring to ISO/IEC 27001 by DANAK (the Danish Accreditation Fund) or a similar accreditation body, who is co-signer of EA's (European co-operation for Accreditation) multilateral agreement with regard to certification of management systems or for certification bodies outside EA's jurisdiction by an accreditation body, who is co-signer of the relevant multilateral agreement on reciprocal recognition under IAF (International Accreditation Forum).

A certification in accordance with a valid ISO/IEC 27001 of a supplier can also replace certification in accordance with The Danish Gambling Authority's Information security management system SCP.03.00.

It is a requirement that the combined scope of the license holder and supplier's ISO/IEC 27001 certifications encompass the entire gambling system as defined in the Danish legislation, as well as any process related to the gambling system and all physical locations of the gambling system.

The accredited testing organisation must have access to the following to be able to assess whether the above conditions are met:

- Valid ISO/IEC 27001 Accreditation/Certification,
- Statement of Applicability, and
- Risk assessment.

On this basis the accredited testing organisation can issue certification which supplants a certification in accordance with Danish Gambling Authority´s Information security management system SCP.03.00.EN.

Guidance: It is not possible for the license holder to be covered by, that one or more suppliers have a ISO/IEC 27001 accreditation.

2.3 Accredited testing organisations

To ensure that the necessary qualifications are in place during the certification the testing organisation and their staff shall fulfil the requirements in this section.

2.3.1 Requirements for accredited testing organisations

Certification in accordance with the information security management system shall be conducted as an accredited certification by a certification body, who is accredited after ISO/IEC 17021-1 or ISO/IEC 17065 for certification referring to Spillemyndighedens Certification Programme SCP.03.00.DK by DANAK (the Danish Accreditation Fund) or a similar accreditation body, who is co-signer of EA's (European co-operation for Accreditation) multilateral agreement with regard to certification of management systems or by certification bodies outside EA's jurisdiction, who is co-signer of the relevant multilateral agreement on reciprocal recognition under IAF (International Accreditation Forum).

Documentation for the accreditation shall be enclosed with the certification. Alternatively, a link to the accreditation can be provided in the certification report.

2.3.2 Requirements for personnel who performs the certification work

The certification work shall be carried out by staff with sufficient qualifications cf. section 6 in ISO/IEC 17021-1 or section 6 in ISO/IEC 17065, which means that the accredited testing organisation shall hire sufficiently qualified, competent, and experienced personnel.

2.3.3 Requirements for personnel who supervise and attest the certification

Work done in relation to the certification shall be supervised and the declaration of certification shall be attested by one or more persons who warrant(s) that the work has been carried out to adequate professional standards. These persons shall meet the following requirements:

a) have a relevant educational background or in other ways prove relevant qualifications,
b) have at least five years of professional experience in inspecting gambling systems and
c) be certified as:
    - International Information Systems Security Certification Consortium (ISC)2 Certified Information Systems Security Professional (CISSP),
    - Information Systems Audit and Control Association (ISACA) Certified Information Systems Auditor (CISA).

See section 2.2 in the general requirements for further information.

3 Requirements for the information security management system

The information security of the licence holder is dependent on the security of the gambling system, the business systems and the business processes dealing with these as well as keeping unauthorised people from getting access to information.

The personnel of the licence holder are important in relation to system access. Therefore their access to both the gambling system and the business systems shall be clearly defined in the terms of employment with the licence holder. This should contribute to limit unauthorised access to the gambling system and business system.

On the technical side a number of operational measures shall be implemented to ensure the integrity of the gambling system and the business systems. In continuation of this, requirements concerning communication channels are also set. Information security shall be incorporated into the development process of the gambling system and business systems to ensure against the corruption of data caused by insufficient validation of the input from other applications.

Third parties can also have access to the gambling system, the business systems or the management system dealing with these if for instance these are suppliers or functions in a role with the licence holder that would require access to the gambling system, business systems or the management system dealing with these.

Regardless of who has access to the gambling system and the business systems, access rights shall be adapted to every individual so access to information is restricted if it is irrelevant for the completion of the duties of said individual.

3.1 Human resource management

The licence holder shall have a policy for the creation, change and termination of user access to the gambling system and the business systems. Based on this policy a formal procedure shall be devised which ensures the following:

- that a detailed job description exist for each staff member,
- that user access to the gambling system and the business systems are in accordance with the job description of each staff member,
- that user access is adapted to reflect any change to the job description, and
- that user access is terminated upon the termination of staff.

Corresponding policies and procedures shall exist in relation to user access to the gambling system and the business systems of consultants and other third parties if such are given access.

3.2 Communications and operations management

3.2.1 Operation procedures and responsibilities

The gambling system and the business systems shall be capable of shutting down safely in the event of a power failure. Emergency power is required to ensure the integrity of data, logs, backups as well as to ensure that on-going games can be concluded.

3.2.2 System planning and monitoring

The gambling system and the business systems shall log system performance and have the facility to provide performance reports.

The use of system resources shall be monitored and adjusted, and projections shall be made of future capacity requirements to ensure adequate system performance.

3.2.3 Protection against malicious code

The gambling system and the business systems shall have tools to detect and prevent intrusion and insertion of unauthorised code.

3.2.4 Backup

The gambling system and the business systems shall have the capacity to backup all critical data and restore all critical data from backup.

The gambling system and the business systems shall be able to recover all critical data from the time of the last backup to the point in time at which the system failure occurred.

3.2.5 Network security management

The gambling system and the business systems shall be implemented in such a way that devices in the same broadcast domain shall not allow any alternate network paths to bypass the firewall.

Firewalls shall be dedicated to firewall operations and shall only contain administrative accounts and firewall related applications.

Firewall access shall be restricted to workstation that are part of the configuration baseline as defined in The Danish Gambling Authority´s change management programme SCP.06.00.EN and shall reject all data packets designated from anywhere else that these workstations.

Firewalls shall maintain an audit log of parameter changes affecting the firewall connection permissions and all successful and unsuccessful access attempts made.

3.2.6 Use of public networks

If the licence holder uses public networks for data traffic between geographically dispersed sub-systems then the information shall be encrypted and the sub-systems shall utilise authentication.

All communications between geographically dispersed sub-systems shall protect against:

- incomplete transmission,
- mis-routing, unauthorised message alteration,
- unauthorised disclosure,
- unauthorised message duplication, og
- unauthorised replay.

The licence holder shall utilise a secure primary DNS and a secure secondary DNS. The secondary DNS shall be logically and physically separate from the primary DNS.

3.2.7 Monitoring

The gambling system and the business systems shall maintain audit logs which record:

- staff members user activities,
- exceptions, and
- information security events.

These audit logs shall be kept for a minimum of five years and be protected against unauthorised access.

The gambling system and the business systems shall record all faults and monitor the use and serviceability of significant components. The significance follows from the classification of components in "Spillemyndigheden's change management programme SCP.06.00.EN."

3.2.8 Time synchronisation

The gambling system and business systems must on a suitable interval undergo time synchronisation through an authoritative time server, that could for instance be used for log entries.

3.3 Access control

The licence holder shall have access control to protect the hardware that supports the systems and the user access to the systems.

3.3.1 Physical access control

There shall be physical access control to the hardware on which the gambling system and the business systems are running, including any other equipment that can access systems.

The level of access control can be adjusted based on the criticality of the systems accessible from the equipment.

3.3.2 User access

The gambling system and the business systems shall enforce the use of strong passwords in relation to user access to the systems as well as timed log-outs or screen savers for inactive access points.

3.3.3 User access management

The authorisation to grant access to the gambling system and the business systems shall be restricted to as few employees as possible. Both the gambling system and the business systems shall allow for user accounts with varying degrees of access and privileges, so the policy and procedure of human resource management cf. section 3.1 can be implemented.

First time passwords shall be changed to a password chosen by the user at the first login.

3.3.4 Network access control and security

The gambling system and the business systems shall enforce access control restrictions on network functions and user access shall only be possible through this access control. The gambling system and the business systems shall prevent unauthorised internal and external access to network functions.

The gambling system and the business systems shall utilised segregated networks so groups of related functions, users and sub-systems are segregated from each other.

3.3.5 Operating system access control and security

All users shall have a unique identifier/user ID for their personal use only and the gambling system and the business systems shall enforce suitable authentication techniques to ensure confirmation of the identity of each user at log in.

Routing controls shall be used to control access to the operating system of significant components. The significance follows from the classification of components in The Danish Gambling Authority´s change management programme SCP.06.00.EN.

When an operating system is installed on a device that is part of the gambling system, only functions that are strictly necessary for the purpose of that device shall be installed/activated. Utilities and programs which might be capable of overriding system and application controls shall never be installed in the gambling system and the business systems of the licence holder.

3.3.6 Application and information access control and security

All users shall have a unique identifier/user ID for their personal use only and the gambling system and the business systems shall enforce suitable authentication techniques to substantiate the claimed identity of each user at log in.

Sensitive information shall be stored and transmitted in an encrypted state and the gambling system and the business systems shall facilitate enhanced access control restrictions to this information.

3.4 Validation of data etc.

3.4.1 Correct processing in applications

Data input to applications shall be validated to ensure that data is context appropriate and unable to harm the gambling system and the business systems.

Automated reconciliation/validation shall be incorporated into applications to ensure against corruption or interference.

Data output from applications shall be validated to ensure that the processing of stored information is correct.

3.4.2 Cryptographic controls and digital signatures

Encryption keys and digital signatures shall be stored in a secure manner.