SC 18032

SSF 1101

For CFPA internal use only

SSF CYBERSECURITY

BASIC LEVEL - BASIC IT SECURITY

SEPTEMBER 2018

Swedish Theft Prevention Association's Norm
SSF 1101 edition 1

SSF
Stöldskyddsföreningen

SSF (the Swedish Theft Prevention Association) is a non-profit association. The aim of the association is to promote safety and security for individuals and property through crime prevention measures, and to help shape opinions and disseminate information with regard to crime prevention. (Excerpt from SSF's by-laws § 1 and § 2. Laid down on May 13, 2011)

SSF, the Swedish Theft Prevention Association, develops and specifies standards for testing and classification within areas considered relevant to the aims of the association.
A list of current SSF standards can be found on the SSF website at www.stoldskyddsforeningen.se

CONTENTS

Foreword

SSF has been publishing rules and standards on behalf of the Swedish Insurance Federation (formerly Försäkringsförbundet) since 2001.

SSF's regulations specify properties that are considered to be of importance for functionality and reliability. The aim of the regulations is to stipulate quality and safety levels that can be applied generally, both when specifying requirements and in conjunction with the procurement of burglar-resistant products or structures.

The regulations refer to, or wherever possible are based on, national and international standards and other applicable technical specifications or international quality standards.

Satisfying statutory requirements can be demonstrated by testing and certification by accredited testing and certification organizations. Products, services, companies and individuals that satisfy applicable standards are listed by SSF in its Security Guide on the SSF website.

Application is voluntary unless agreed otherwise.

In addition to the requirements specified in the standards and regulations, compliance with laws and official regulations is assumed.

Stockholm, September 2018.

Orientation

This standard has been produced by SSF and PwC. The following organizations have participated in the reference group: The police, the Swedish Civil Contingencies Agency (MSB), the Swedish Trade Federation, the Confederation of Swedish Enterprise and SEM Group. This standard specifies basic IT security requirements.

The organizations of today face a number of security-related challenges when it comes to handling, storing and transferring information. This standard is aimed primarily to small and medium-sized organizations that are in need of practical action in order to effectively protect important information as part of their business.

This document constitutes Basic level – basic IT security and should act as a first step in organizations' efforts to enhance the ability to deal with risks linked with information management. This standard aims to specify requirements for certification in accordance with the basic level.

What is information security?
Information security involves preservation of confidentiality, accuracy and availability of information. Information is an asset which, like other important business assets, is of value to businesses and therefore needs appropriate protection. Information security measures aim to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, review, playback or destruction.

1 Scope

This standard includes basic and specific requirements that must be met by small and medium-sized organizations in order to achieve certification in accordance with SSF 1101 – SSF Cybersecurity Basic level – basic IT security.

The scope of certification can be restricted to a specific organizational element and/or a technical function (one or more systems or processes).

2 References

This standard contains dated or undated references to regulations in other publications. These normative references can be found in the body copy. The publications are listed below. With regard to dated references to publications that have subsequently been amended or supplemented, such amendments and supplements are only valid if they have been inserted into these regulations. For undated references, the latest edition of the publication applies.

SS-EN ISO/IEC 17021	*Conformity assessment – Requirements for bodies providing audit and certification of management systems*
SS-EN ISO/IEC 17024	*Conformity assessment – General requirements for bodies operating certification of persons*
DISA	*Computer-aided information security training for users. (2017). Swedish Civil Contingencies Agency (MSB).* *https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/DISA---Datorstodd-informationssakerhetsutbildning-for-anvandare/*

3 Definitions

The definitions, terms and abbreviations specified below are applicable when using this document.

3.1
user account (user)
An account with the minimum access rights possible, this allows the user to do their work and is used for working on tasks that do not relate to system administration.

3.2
application
This refers to a program with the aim of constituting a link between the computer's operating system and the user. Examples of applications are Microsoft Excel, Google Chrome, Adobe Photoshop, Spotify and McAfee Antivirus.

3.3
authorization
Assigned rights to use an information asset in a specified manner. Rights that can be assigned may allow you to read, write, edit or delete information.

3.4
computer
This includes laptop computers, desktop computers, servers or similar.

3.5
mobile devices
This includes mobile phones, tablets and wearables (e.g. smartwatches) or similar.

3.6
network device
This includes routers, firewalls, manageable switches and suchlike. It also includes all devices – with the exception of guest devices on the guest network – that are connected to the organization's network and that are not specified under 3.3 computer or 3.4 mobile devices. Networked CCTV cameras, printers and smart devices are examples of this.

3.7
organization's resources
These are resources that are owned or managed by the organization within the organization's infrastructure/environment.

3.8
operating system
This refers to one or more programs with the aim of constituting a link between the computer’s hardware and the user’s software. Windows 7/8/10, Linux and Mac OS X are examples of this.

3.9
portable storage media
This refers to USB sticks, external hard disks, CDs and DVDs or similar.

3.10
software
This refers to software in the sense of an organized collection of data and machine instructions which execute tasks in a computer system. This includes both operating systems and applications, but also programming tools under the programs that come within the definitions above.

3.11
service accounts
Service accounts are accounts that are not used by administrators or users, but by services that need an account for access purposes, for example. An account belonging to a database service that needs write rights to a server or an account belonging to an antivirus program that needs to be able to read users' files are examples of this.

3.12
strong passwords
A strong password must not appear in known password dumps/password lists and contain at least 10 characters. Passwords must be made up of upper and lower case letters and special characters and not include a word that appears in a dictionary or similar where substitution has occurred (e.g. replacing a letter in a word with a digit).

4 Requirements

4.1 Computers and mobile devices

4.1.1 General:

- default passwords for user accounts for computers and mobile devices must be changed to strong passwords that are not reused

  Note No passwords are to be reused (this includes both passwords used previously and using the same password on different devices) by either employees or groups of employees.

  Passwords that have been used within the organization must not be used privately, or vice versa.

- strong passwords must be defined in a decision by the organization. As a minimum, passwords must comply with the security level as specified in the standard
- encryption of storage space on computers and mobile devices must be enabled wherever possible.

4.1.2 Creating backups

- information must be backed up to the extent decided upon by the company
- At least one backup must be available only to individuals with administrative system access rights.

  Note Information backed up may be checked by carrying out regular random inspections.

4.1.3 Protection against malicious code

Software for protection against malicious code:

- must be installed on all computers and mobile devices that are or may be connected to external networks such as the Internet
- must be updated automatically or by means of a special procedure
- must be configured to automatically search files on arrival (including when downloading and opening files on network devices and portable storage media)
- must scan websites on computers and alert the user if the website contains malicious code

  Note The software must use warnings or blocking to ensure that the user's attention is drawn to websites that contain malicious code and prevent the code being executed initially.

- must be configured to execute regular scans for malicious code

4.1.4 Use of the organization's resources for private use

- decisions must be made on whether the organization's resources may be used for private use, and if so to what extent.

4.1.5 Use of private equipment

- decisions must be made on whether private equipment may be used within the organization, and if so to what extent.
- private equipment used within the organization must be subject to the same security requirements as the rest of the organization's equipment.

4.2 Software and applications

4.2.1 General

- all software that is subject to copyright must be licensed for use within the organization
- if possible, software must always be downloaded from the official distributor's website or similar verifiable sources
- applications for mobile devices must only be downloaded from trusted sources
- only software and applications that are necessary for the business are to be installed

  Note See section 4.1.4
- software and applications that are not used must be uninstalled as soon as possible.

  Note Downloading applications to mobile phones and tablets from trusted sources involves the AppStore, Google Play Store or the organization's own internal site for approved programs and applications, for example.

4.2.2 Security updates

- security updates must be installed automatically for operating systems, software and applications that run on computers, network devices and mobile devices, where technically possible
- operating systems, software, applications and network devices for which security updates are no longer installed must be removed or moved to logically or physically separated segments where they can be managed on the basis of special rules.

  Note If this requirement is not met, the organization must justify why it accepts the risk of deviating from the above requirement.

4.2.3 Automatic program launch and automatic playback

- automatic program launch must be limited to applications that are identified by the organization as being necessary to launch automatically

  Note Decisions on the applications identified must be made by the organization.
- automatic playback must be disabled for all files from portable storage media.

4.3 Networks

4.3.1 General

- one or more network devices with firewall functionality must be installed between the company's internal network and external networks such as the Internet

  Note If there is no internal network, computers must be provided with firewall functionality between computers and external networks such as the Internet.

- before a network device is installed, the default password must be changed to a strong password that is not reused, where technically possible

  Note No passwords are to be reused (this includes both passwords used previously and using the same password on different devices) by either employees or groups of employees.

  Passwords that have been used within the organization must not be used privately, or vice versa.

- passwords for administrative accounts (including service accounts) on network devices must be changed at intervals decided upon by the organization
- all open connections (i.e. permitted ports and services) in the firewall must be decided upon by the organization.

  Note This decision should be documented (including an explanation of the needs of business)

- firewall rules that are no longer needed must be deleted or disabled
- computers that do not need to connect to the Internet must be prevented from initiating connections to the Internet
- the administrative interface used to configure the organization's firewall or firewalls must not be accessible from external networks such as the Internet
- all wireless networks must be encrypted and protected by a secure protocol, and with a strong password or certificate.

  Note A secure protocol is a protocol in line with prevailing good practice. WPA2-PSK(AES) or equivalent is recommended at present.

4.3.2 Guest network

- the guest network must be separated from the organization's internal network

Note 1. The password for the guest network will only be disclosed to authorized persons.

Note 2. Regular work must not take place via the guest network.

4.3.3 Traffic protection

- when using public networks (such as public Wi-Fi and wired public networks), traffic must be protected from unauthorized access by means of a VPN or similar
- communication between client and server for email must be protected with encryption

  Note Encryption may take place with the help of TLS (Transport Layer Security).
- the organization's domain name for DNS must be protected with DNSSEC.

4.4 External IT services, including cloud storage

4.4.1 Agreement

- there must be a legally binding agreement between the organization and the supplier when using external IT services and cloud services

4.4.2 Scope of the agreement

The agreement should normally include the following terms:

- who owns the information
- who has access to the information
- where the information is stored (geographically)
- which service level (accessibility, support, troubleshooting, etc.) the organization can expect from the supplier and agreed deliveries (availability on the Internet, for example)
- the fact that the supplier has a security level through accreditations, certificates or other independent evidence that corresponds to or surpasses the requirements in accordance with this standard
- how security incidents are handled by the supplier and reported to the client
- the fact that information is backed up and how data recovery takes place
- if information is encrypted, and if so how

4.4.3 GDPR

- if the service includes processing or storage of personal data, the supplier must certify that it is compliance with requirements in accordance with the European General Data Protection Regulation (GDPR)
- a personal data assistant agreement must exist between the supplier and the organization if so required

4.5 Access rights

4.5.1 User accounts

- user accounts must be created following decisions by the organization

  Note These decisions should be documented.

- system administrator access rights may only be assigned and used by individuals performing system administration tasks
- administrative accounts must only be used to implement permitted administrative activities such as system maintenance
- user accounts must be assigned to individual employees
- user accounts must be deleted or disabled when they are no longer needed (e.g. when an employee changes role or leaves the organization).

4.5.2 Access

- individual employees must only have access to the systems required by their work
- shared storage areas must be configured so that individual employees can only access the information required by their work

4.5.3 Passwords

- as a minimum, users must be authenticated using strong passwords that are not reused before access to programs and computers will be permitted
- passwords for system administrator accounts and service accounts must be changed at intervals decided upon by the organization
- if it is suspected or can be demonstrated that a password has been disclosed to anyone other than the user themselves, it must be changed immediately
- passwords must be changed to the extent and at the intervals required by the business

4.6 Information security training

All employees must complete basic training on information security in the form of DISA – Computer-aided information security training for users (Swedish Civil Contingencies Agency, MSB) or training with a similar scope.

5 Requirements for certification bodies

5.1 Organization

The certification body must be a registered legal entity within the European Union (EU) or the European Economic Area (EEA).

5.2 Accreditation

The certification body must be accredited by SWEDAC or another full member of the EA (European co-operation for Accreditation) for certification in accordance with ISO/IEC 17021 and ISO/IEC 17024.

5.3 Certificates

Certificates will be issued when all requirements in accordance with this standard have been met. The maximum period of validity of 3 years.

Certificates issued must be revoked without unnecessary delay when:

- inspections show that the organization has serious shortcomings in relation to defined requirements and if shortcomings reported are not rectified
- the certification body receives information that directly justifies revocation, e.g. with regard to bankruptcy, bankruptcy application, initiated reconstruction or the organization is otherwise considered insolvent.

Bibliography

The following standards and documents have been used as a basis for the standard:

SS-EN-ISO/IEC 27001:2017	*Information technology – Security techniques – Information security management systems – Requirements.*
SS-EN-ISO/IEC 27002:2017	*Information technology – Security techniques – Code of practice for information security controls.*
SIS – TR 50:2015	*Terminologi för Informationssäkerhet*
MSB1138	*Informationssäkerhet för småföretag. Praktiska råd och rekommendationer. Swedish Civil Contingencies Agency*
NIST	*Digital Identity Guidelines (2017), NIST – National Institute of Standards and Technology.*
National Cyber Security Centre	*NCSC, Cyber Essentials.*

ISBN 978-91-88191-18-2

This standard can be ordered from:
www.stoldskyddsforeningen.se
Tel +46 8 783 75 33

SSF
Stöldskyddsföreningen