

SSF 1101

REGULATIONS FOR

SSF CYBERSECURITY

BASIC LEVEL – BASIC IT SECURITY

DECEMBER 2023

SSF 1101 Edition 2

SSF Swedish Theft Prevention Association (SSF) is a non-profit organisation whose purpose is to promote safety and security for businesses, people and property through crime prevention, and to act as a former of opinion and information disseminator in crime prevention ([SSF's statutes](#)).

SSF publishes regulations and norms that specify quality and security levels in burglary resistance and IT security that are recommended for application for products, people and businesses. SSF has been publishing rules and norms on behalf of Insurance Sweden since 2001.

The basic purpose of the norm work is to help prevent and limit the extent of damage, thereby reducing the cost of damage. Another aim is to provide clarity for stakeholders in the security industry and customers of insurance companies. In addition to the requirements specified in the norms and rules, compliance with laws and official regulations is assumed.

A current list of SSF norms can be found at www.stoldskyddsforeningen.se.

SSF offers a number of services to help facilitate the application of norms.

Participate in the development and revision of norms.

Participating in SSF's working groups for development of norms gives you the opportunity to influence work on issues that are important for your organisation, and for national security work in general.

SSF Norm subscription

SSF Norm subscription gives you quick and easy access to relevant standards and news in your field of work.

Training and advice

SSF offers training and advice based on our norms to help and support you in your day-to-day work.

Contact

info@stoldskyddsforeningen.se

Copyright © 2023 SSF Swedish Theft Prevention Association.

Contents

ORIENTATION..... 4

1 SCOPE..... 5

2 REFERENCES..... 5

3 DEFINITIONS..... 5

4 REQUIREMENTS..... 7

4.1 COMPUTERS AND MOBILE DEVICES 7

4.2 SOFTWARE AND APPLICATIONS 8

4.3 NETWORKS 9

4.4 IT SERVICES..... 10

4.5 PERMISSIONS..... 10

4.6 CYBERSECURITY TRAINING 11

5 REQUIREMENTS FOR CERTIFICATION BODIES 11

5.1 ORGANISATION..... 11

5.2 ACCREDITATION 11

5.3 CERTIFICATES 11

ANNEX A (INFORMATIVE) CLOUD SERVICES – IT SERVICES..... 12

ANNEX B (INFORMATIVE) BIBLIOGRAPHY 13

Orientation

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

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

It is important that everyone in an organisation to be aware of and understand the content of policies and guidelines. Experience clearly shows the importance of employees demonstrating safe behaviour in their day-to-day work.

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

Cybersecurity

Cybersecurity refers to the protection of systems, networks and software from digital attacks, damage and unauthorised access. It includes technical, organisational and behavioural measures to protect information, data and technological resources from threats that may arise in cyberspace.

Employees' digital identities are the key to the organisation's most sensitive information. That is why cyber attacks are increasingly focused on gaining access to permissions.

Updates from the previous edition:

- Updated references
- Updated definitions
- IT services
- Clearer recommendations regarding passwords
- Multi-factor authentication
- Changed educational requirements

SSF 1101 edition 2 is valid from 6 December 2023.

SSF 1101 edition 1 will be suspended on 31 December 2024.

1 Scope

This norm includes basic and specific requirements that must be met by small and medium-sized organisations 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 organisational element and/or a technical function (one or more systems or processes).

2 References

The following publications include requirements which, in part or in full, constitute requirements in this norm.

Only the listed edition applies in the case of dated references.

The latest edition of the publication, including any published interpretations and additions, applies in the case of undated references.

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 that certify persons*

3 Definitions

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

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.

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.

authorisation

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.

computer

this includes laptop computers, desktop computers, servers or similar.

mobile devices

this includes mobile phones, tablets (computers with mobile operating systems) and wearables (e.g. smartwatches) or similar.

cloud services

are systematic computing services – including storage, computing, networking, databases and analytics – delivered via the internet (“the cloud”), and often provided on demand and based on actual usage. See the main categories in Annex A.