SSF 1101

NORM AVSEENDE

SSF CYBERSÄKERHET

BASNIVÅ - GRUNDLÄGGANDE IT-SÄKERHET

OKTOBER 2023

SSF 1101 utgåva 2

SSF
Stöldskyddsföreningen

SSF Stöldskyddsföreningen (SSF) är en ideell förening som har till ändamål att främja trygghet och säkerhet för verksamhet, person och egendom genom förebyggande arbete mot brott samt att verka som opinionsbildare och informationsspridare i det brottsförebyggande arbetet (SSF:s stadgar in Swedish).

SSF ger ut regelverk och normer vilka specificerar kvalitets- och säkerhetsnivåer inom inbrottssäkerhet och IT-säkerhet som rekommenderas att tillämpas för produkter, personer och företag. Sedan 2001 är SSF utgivare av regler och normer på uppdrag av Svensk Försäkring.

Det grundläggande syftet med normarbetet är att bidra till att förebygga och begränsa skadors omfattning, och därmed ge lägre skadekostnader. Syftet är också att skapa en tydlighet för aktörer i säkerhetsbranschen och för försäkringsbolagens kunder. Utöver de krav som är angivna i normerna och reglerna förutsätts att lagar och myndighetsföreskrifter följs.

Aktuell förteckning över SSF:s normer återfinns på www.stoldskyddsforeningen.se.

SSF erbjuder flera tjänster för att underlätta vid tillämpningen av normer.

Delta vid framtagning och revidering av normer

Genom att delta i SSF:s arbetsgrupper för normframtagning har du möjlighet att påverka arbetet i frågor som är viktiga för din organisation och för det nationella säkerhetsarbetet i stort.

SSF Norm Subscription

Med SSF Norm Subscription får du snabb och enkel tillgång till relevanta normer och nyheter inom ditt arbetsområde.

Utbildning och rådgivning

Baserat på våra normer erbjuder SSF utbildning och rådgivning som hjälper och stödjer dig i ditt dagliga arbete.

Kontakt

info@stoldskyddsforeningen.se

INNEHÅLL

Förord

Sedan 2001 är SSF Stöldskyddsföreningen utgivare av regler och normer på uppdrag av Svensk Försäkring (tidigare Försäkringsförbundet).

SSF Stöldskyddsföreningens regelverk anger egenskaper som anses vara av betydelse för funktion och tillförlitlighet. Avsikten med regelverken är att lägga fast kvalitets- och säkerhetsnivåer som kan tillämpas generellt vid såväl specificering av krav som i samband med upphandling av inbrottsskyddande produkter eller konstruktioner.

Regelverken refererar till, eller bygger så långt som möjligt på, nationella och internationella standarder samt andra tillämpliga tekniska specifikationer eller kravdokument.

Att kraven i ett regelverk är uppfyllda kan visas genom provning och certifiering hos ackrediterade provnings- och certifieringsorgan.

Tillämpningen är frivillig om inget annat avtalats.

Utöver de krav som är angivna i normerna och reglerna förutsätts att lagar och myndighetsföreskrifter följs.

Stockholm i oktober 2023.

Orientering

Denna norm är framtagen av SSF och PwC. I referensgruppen har följande organisationer deltagit: Polisen, Myndigheten för samhällsskydd och beredskap (MSB), Svensk Handel, Svenskt Näringsliv, SEM Group. Normen specificerar krav på grundläggande it-säkerhet.

Dagens organisationer har flera säkerhetsrelaterade utmaningar när det kommer till att hantera, lagra och överföra information. Denna norm riktar sig främst till små och medelstora organisationer som är i behov av praktiska åtgärder för att effektivt skydda viktig information i sin verksamhet.

Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.

Detta dokument utgör Basnivå – grundläggande it-säkerhet och ska fungera som ett första steg i organisationers arbete att höja förmågan att möta risker kopplat till informationshantering. Normen syftar till att specificera krav på certifiering enligt basnivån.

Cybersäkerhet
Cybersäkerhet avser skyddet av system, nätverk och program från digitala attacker, skador och obehörig tillgång. Det innefattar tekniska, organisatoriska och beteendemässiga åtgärder för att skydda information, data och teknologiska resurser från hot som kan uppstå i cyberrymden.

Medarbetarnas digitala identiteter är nyckeln till verksamhetens mest känsliga information. Därför fokuserar cyberattacker allt oftare på att komma åt just behörigheter.

Uppdateringar från föregående utgåva:
- Uppdaterade referenser
- Uppdaterade definitioner
- IT-tjänster
- Tydligare rekommendationer angående lösenord
- Multifaktorsautentisering
- Ändrade utbildningskrav

SSF 1101 utgåva 2 gäller från 1 december 2023.
SSF 1101 utgåva 1 dras in 2024-12-31.

1 Omfattning

Denna norm innehåller grundläggande och konkreta krav som ska uppfyllas av små och medelstora organisationer för att kunna erhålla certifiering enligt SSF 1101 – SSF Cybersäkerhet Basnivå - grundläggande it-säkerhet.

Omfattningen av certifieringen kan avgränsas till en viss organisatorisk del och/eller en teknisk funktion (ett eller flera system eller processer).

2 Referenser

Denna norm innehåller daterade eller odaterade hänvisningar till regler i andra publikationer. Dessa normativa hänvisningar återfinns i den löpande texten. Publikationerna anges nedan. Beträffande daterade hänvisningar till publikationer som senare har ändrats eller fått tillägg, gäller dessa ändringar eller tillägg endast då de har införts i dessa regler. Vid odaterade hänvisningar gäller den senaste utgåvan av publikationen.

SS-EN ISO/IEC 17021	*Bedömning av överensstämmelse - Krav på organ som reviderar och certifierar ledningssystem*
SS-EN ISO/IEC 17024	*Bedömning av överensstämmelse – Allmänna krav på organ som certifierar personer*

3 Definitioner

För tillämpning av detta dokument gäller de definitioner, termer och förkortningar som anges nedan.

användarkonto (user)
konto med minsta möjliga behörigheter, för att lösa sina arbetsuppgifter och som används för arbete i icke-systemadministrativa sysslor.

applikation
avser ett program som syftar till att utgöra länken mellan datorns operativsystem och användaren. Exempel på detta är Microsoft Excel, Google Chrome, Adobe Photoshop, Spotify och McAfee Antivirus.

behörighet
tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt. Exempel på rättigheter som kan tilldelas är att läsa, skapa, ändra eller ta bort information.

dator
avser såväl bärbara datorer, stationära datorer som servrar eller motsvarande.

mobila enheter
avser såväl mobiltelefoner, surfplattor (datorer med mobila operativsystem) som wearables (t.ex. smarta klockor) eller motsvarande.

molntjänster
är systematiska datortjänster – inklusive lagring, beräkning, nätverk, databaser och analyser – som levereras via internet ("molnet") och som ofta tillhandahålls på begäran och baseras på den faktiska användningen. Se huvudkategorier i Bilaga A.

multifaktorsautentisering (MFA)
innebär att det krävs minst två, av varandra oberoende, inloggningsfunktioner.

nätverksenhet
avser routrar, brandväggar, managerbara switchar och motsvarande. Det avser också alla interna nätverksenheter, undantaget gästenheter i gästnätverket, som är anslutna till organisationens nätverk och som inte är specificerade under definitionerna dator eller mobila enheter. Exempel på detta är nätverksanslutna övervakningskameror, skrivare, och smarta enheter.

operativsystem
avser ett eller flera program som syftar till att utgöra länken mellan datorns hårdvara och användarens programvara, gäller även mobila operativsystem.

organisationens resurser
avser resurser som ägs eller hanteras av organisationen i organisationens infrastruktur/miljö.

portabla lagringsmedier
avser USB-minnen, externa hårddiskar, CD- och DVD-skivor eller motsvarande.

programvara
avser mjukvara i betydelsen organiserad samling av data och maskininstruktioner vilka utför en uppgift på ett datorsystem. I detta inkluderas både operativsystem och applikationer, men även programmeringsverktyg och andra program som faller utanför definitionerna ovan.

servicekonton
avser konton som varken används av administratörer eller användare, utan av tjänster som behöver ett konto för exempelvis tillgång. Exempel på detta är ett konto tillhörande en databastjänst som behöver skrivrättigheter på en server eller ett konto tillhörande ett antivirusprogram som behöver kunna läsa användares filer.

starka lösenord
består av minst 12 tecken, lösenordet kan bestå av en kombination av versaler, gemener, siffror och symboler. Får ej vara ett ord som finns i en ordlista eller namnet på en person, tecken, produkt, organisation eller förekomma i kända lösenordsdumpar/lösenordslistor.

4 Krav

4.1 Datorer och mobila enheter

4.1.1 Allmänt:

- standardlösenord för alla användarkonton till datorer, mobila enheter och on-line konton ska ändras till starka lösenord som inte återanvänds.
- inga lösenord ska återanvändas (gäller såväl tidigare använda lösenord som användande av samma lösenord på olika enheter) av vare sig medarbetare eller grupper av medarbetare.
- lösenord som använts inom organisationen ska inte användas privat, eller vice versa.
- starka lösenord ska vara definierade i ett beslut av organisationen. Lösenord ska minst uppfylla säkerhetsnivån enligt denna norm.
- kryptering av lagringsutrymme på datorer, mobila enheter och digitala lagringsutrymmen ska vara aktiverade där så är möjligt.

4.1.2 Säkerhetskopiering

- information ska säkerhetskopieras i den omfattning verksamheten beslutat.
- minst en säkerhetskopia ska vara tillgänglig endast för personer med administrativ systembehörighet.

  Anm. Kontroll av säkerhetskopierad information ska ske genom regelbundna stickprovskontroller.

4.1.3 Skydd mot skadlig kod

Programvara för skydd mot skadlig kod:

- ska vara installerad på alla datorer och, där så är möjligt, på mobila enheter som är anslutna till eller kan ansluta till externa nätverk, t.ex. Internet.
- ska uppdateras automatiskt eller genom särskild rutin.
- ska vara konfigurerad för att automatiskt genomsöka filer vid åtkomst (inklusive vid hämtning och öppning av filer på nätverksenheter och flyttbara lagringsmedia).
- ska på datorer skanna och varna om webbplatsen innehåller skadlig kod.

  Anm. Programvaran ska genom varning eller blockering säkerställa att användaren uppmärksammas på webbsidor som innehåller skadlig kod, och förhindra att koden exekveras i ett initialt skede.
- ska vara konfigurerad för att genomföra regelbundna skanningar efter skadlig kod.

4.1.4 Användning av organisationens resurser för privat bruk

Det ska vara beslutat om och i vilken omfattning organisationens resurser får användas för privat bruk.

Anm. All användning av organisationens resurser för privat bruk kan utgöra en säkerhetsrisk.

4.1.5 Användning av privat utrustning

- det ska vara beslutat om och i vilken omfattning privat utrustning får användas i organisationens verksamhet.
- privat utrustning som används i organisationen ska omfattas av samma säkerhetskrav som organisationens utrustning i övrigt.

4.2 Mjukvaror och applikationer

4.2.1 Allmänt

- all mjukvara, ska vara licensierad för användning i organisationens verksamhet.
- mjukvara, ska om möjligt alltid laddas ned från den officiella distributörens hemsida eller liknande verifierbara källor.
- applikationer till mobila enheter får endast laddas ned från betrodda källor.
- mjukvaror och applikationer som inte används ska avinstalleras så snart som möjligt.

  Anm. Att ladda ner applikationer till mobiltelefoner och surfplattor från betrodda källor innebär exempelvis AppStore, Google Play Store eller organisationens egen interna plats för godkända program och applikationer.

4.2.2 Säkerhetsuppdateringar

- säkerhetsuppdateringar ska installeras automatiskt för operativsystem, programvaror och applikationer som körs på datorer, nätverksenheter och mobila enheter, där det är tekniskt möjligt.
- operativsystem, programvaror, applikationer och nätverksenheter som inte längre säkerhetsuppdateras ska tas bort eller flyttas till logiskt eller fysiskt separerade segment där de kan hanteras utifrån särskilda regler.

  Anm. Om kravet inte uppfylls ska organisationen motivera varför man accepterar risken med att frångå ovanstående krav.

4.2.3 Automatisk programstart och automatisk uppspelning

- automatisk programstart ska vara begränsat till applikationer som är identifierade av organisationen som nödvändiga att starta automatiskt.

  Anm. De identifierade applikationerna ska vara beslutade av organisationen.
- automatisk uppspelning ska vara avstängt för alla filer från portabla lagringsmedier.

4.3 Nätverk

4.3.1 Allmänt

- en eller flera nätverksenheter med brandväggsfunktionalitet ska vara installerade mellan företagets interna nätverk och externa nätverk t.ex. internet.

  Anm. I de fall det inte finns ett internt nätverk ska datorer vara försedda med brandväggsfunktionalitet mellan dator och externa nätverk, t.ex. Internet.

- innan en nätverksenhet installeras ska standardlösenordet ändras till ett starkt lösenord som inte återanvänds, där så är tekniskt möjligt.
- lösenordsändringar för administrativa konton (inklusive servicekonton) i nätverksenheter ska ske enligt intervall beslutade av organisationen.
- alla öppna anslutningar (dvs. tillåtna portar och tjänster) på brandväggen ska vara beslutade av organisationen.
- brandväggsregler som inte längre behövs ska tas bort eller inaktiveras.
- enheter som inte behöver ansluta till Internet ska förhindras från att initiera anslutningar till Internet.
- det administrativa gränssnittet som används för att konfigurera organisationens brandvägg eller brandväggar ska inte vara åtkomligt från externa nätverk, t.ex. Internet.
- samtliga trådlösa nätverk ska vara krypterade och skyddas av ett säkert protokoll och med ett starkt lösenord eller certifikat.

  Anm. Med säkert protokoll avses ett protokoll i linje med rådande god sed. För närvarande rekommenderas som lägst WPA2-PSK (AES) eller motsvarande.

4.3.2 Gästnätverk

Ska vara avskilt från organisationens interna nätverk.

Anm 1. Lösenordet till gästnätverket delges enbart behöriga.

Anm 2. Ordinarie arbete ska inte ske via gästnätverket.

4.3.3 Trafikskydd

- vid användande av allmänna nätverk (så som offentligt Wi-Fi och trådbundna allmänna nätverk) ska trafiken skyddas från obehörig insyn med hjälp av VPN eller motsvarande.
- kommunikation mellan klient och servrar för e-post ska vara skyddad med kryptering.

  Anm. Kryptering kan ske med hjälp av TLS (Transport Layer Security).

- organisationens domännamn för DNS ska skyddas med DNSSEC.

4.4 IT-tjänster

- organisationen ska identifiera de leverantörer vilkas it-tjänster är kritiska för organisationens verksamhet. Se bilaga A IT-tjänster.
- organisationen ska säkerställa att de leverantörer vilkas it-tjänster är kritiska för organisationens verksamhet har en grundläggande cybersäkerhet.
- leverantörens nivå av cybersäkerhet ska säkerställas genom egendeklaration, ackrediteringar, intyg, certifikat eller motsvarande.
- det ska finnas ett juridiskt bindande avtal mellan organisationen och identifierade leverantörer av kritiska it-tjänster.

4.4.1 **Avtalet ska normalt omfatta följande villkor**:

- vilken servicenivå (tillgänglighet, support, felavhjälpning etc.) organisationen kan förvänta sig av leverantören och avtalade tjänsteleveranser.
- hur säkerhetsincidenter hanteras av leverantören och rapporteras till beställaren.
- att informationen säkerhetskopieras och hur återställning genomförs.
- om och på vilket sätt informationen krypteras.
- åtgärder och ansvar vid avtalets upphörande.

4.4.2 GDPR

- i det fall tjänsten omfattar behandling eller lagring av personuppgifter ska leverantören intyga att denne uppfyller kraven enligt den europeiska dataskyddsförordningen (GDPR).
- ett personuppgiftsbiträdesavtal ska finnas mellan leverantören och organisationen om detta så krävs.

4.5 Behörigheter

4.5.1 Användarkonton

- skapande av användarkonton ska ske efter beslut av organisationen.

  Anm. Beslutet bör vara dokumenterat.

- systemadministratörsbehörighet får endast tilldelas och användas av personer som utför systemadministrativa tjänster.
- administrativa konton ska endast användas för att utföra tillåtna administrativa aktiviteter, t.ex. systemunderhåll.
- användarkonton ska vara tilldelade enskilda medarbetare.
- användarkonton ska tas bort eller inaktiveras när de inte längre behövs (t.ex. när en medarbetare ändrar roll eller lämnar organisationen).

4.5.2 Åtkomst

- enskilda medarbetare ska endast ha åtkomst till de system som arbetsuppgifterna kräver.
- delade lagringsytor ska vara konfigurerade så att enskilda medarbetare endast har åtkomst till den information arbetsuppgifterna kräver.

4.5.3 Lösenord och multifaktorsautentisering (MFA)

- användare ska, som minimum, autentiseras med starka lösenord som inte återanvänds, innan åtkomst beviljas till program och datorer.
- i samtliga fall det är tekniskt möjligt ska multifaktorautentisering (MFA) användas för autentisering av användare.
- lösenordsändringar för systemadministratörskonton och servicekonton ska ske enligt intervall beslutade av organisationen.
- om det misstänks eller kan konstateras att lösenord har blivit känt för någon annan än användaren själv ska det omedelbart bytas ut.
- lösenord ska bytas ut i den omfattning och med den regelbundenhet som verksamheten kräver.

4.6 Utbildning i cybersäkerhet

Samtliga medarbetare ska genomföra grundläggande utbildning i cybersäkerhet. Utbildningen ska minst omfatta;

- hot, risker och säkert beteende.
- i utbildningen ska ingå områden som lösenordshantering, säkerhetskopiering, molntjänster, e-post, sociala medier, skadlig kod, distansarbete, när en incident inträffar och hantering av mobila enheter.

5 Krav på certifieringsorgan

5.1 Organisation

Certifieringsorganet ska vara registrerad juridisk person inom den Europeiska unionen (EU) eller den europeiska frihandelssammanslutningen (EES).

5.2 Ackreditering

Certifieringsorganet ska vara ackrediterat av SWEDAC eller annan fullvärdig medlem av EA, (European co-operation for Accreditation) för certifiering enligt ISO/IEC 17021 och ISO/IEC 17024.

5.3 Certifikat

Certifikat utfärdas då samtliga krav enligt denna norm är uppfyllda. Giltighetstiden är längst 3 år.

Utfärdat certifikat ska återkallas utan onödigt dröjsmål då:

- kontroll visar att organisationen har allvarliga brister i förhållande till ställda krav och om påtalade brister inte åtgärdas.
- certifieringsorganet får del av information som direkt motiverar återkallande t.ex. gällande konkurs, konkursansökning, inledd rekonstruktion eller organisationen på annat sätt anses ha kommit på obestånd.

Bilaga A (Informativ) Molntjänster – IT tjänster

Molntjänster kan grovt delas in i tre huvudkategorier:

- **Infrastructure as a Service (IaaS):**
  Denna tjänst erbjuder grundläggande infrastruktur tjänster till användaren, till exempel rå beräkningskraft, lagringsutrymme och nätverkskapacitet. Användaren kan sedan installera egen programvara och applikationer på den tillhandahållna infrastrukturen.

- Platform as a Service (PaaS):
  PaaS erbjuder en utvecklingsmiljö till användare. Ovanpå den underliggande lagringen och nätverksinfrastrukturen tillhandahåller PaaS en hel uppsättning verktyg och tjänster som gör det möjligt för utvecklare att bygga, testa och driftsätta applikationer utan att behöva oroa sig för den underliggande infrastrukturen.

- **Software as a Service (SaaS):**
  Detta är den mest kända kategorin av molntjänster. Med SaaS levereras en hel applikation till slutanvändaren. I stället för att köpa och installera särskild programvara på enskilda datorer eller servrar i ett nätverk, kan användaren helt enkelt använda programmet via internet, oftast genom en webbläsare.

IT-tjänster

Exempel på kritiska it-tjänster, system som hanterar;

- överföringar, betalningar, bokföring och andra kritiska finansiella transaktioner, företagsresurssystem (ERP) och kundrelationshantering (CRM),
- e-handelsplattformar som behandlar beställningar och betalningar,
- elektroniska patientjournaler,
- studieadministrativa system,
- kommunikationssystem för samhällsviktiga funktioner,
- system för larmöverföring,
- system för brand- och säkerhetslösningar,
- skatteadministrativa system,
- kontrollsystem för energidistribution, vatten- och avloppsbehandlingssystem, transportledningssystem för flyg, tåg och andra transportmedel,
- telekommunikationsnätverk och tjänster, inklusive mobilnät och internetaccess, säkerhetslösningar,
- drift av webbplats, tjänster för fil- och dokumenthantering, databackup och återställning,
- e-postsystem och relaterade tjänster,
- molntjänster som lagrar och hanterar kritisk information och tjänster

Bilaga B (Informativ) Bibliografi

Som underlag till normen har följande standarder och dokument använts:

SS-EN-ISO/IEC 27001:2017	*Informationsteknik – Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav.*
SS-EN-ISO/IEC 27002:2017	*Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder.*
SIS - TR 50:2015	*Terminologi för Informationssäkerhet*
MSB	*Terminologi för cybersäkerhet*
MSB1138	*Informationssäkerhet för småföretag. Praktiska råd och rekommendationer. Myndigheten för samhällsskydd och beredskap*
NIS/NIS 2	*Krav på informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga- och vissa digitala tjänster.*
NIST	*Digital Identity Guidelines (2017), NIST - National Institute of Standards and Technology.*

National Cyber Security Centre *NCSC, Cyber Essentials*

ISBN 978-91-88191-70-0

Denna skrift beställs på:
stöldskyddsföreningen.se
Tel 0771-773 773

SSF
Stöldskyddsföreningen