

Spillemyndighedens certifieringsprogram for væddemål og onlinekasino



Ledelsessystem for informationssikkerhed –
SCP.03.00.DK.3.0

Indholdsfortegnelse

1.	Formålet med ledelsessystem for informationssikkerhed	2
1.1	Version	3
1.2	Anvendelsesområde	3
2.	Frekvens og testvirksomheder	4
2.1	Certificeringsfrekvens	5
2.1.1	Første certificering	5
2.1.2	Fornyset certificering	5
2.1.3	Udsættelse af fornyset certificering	5
2.2	Certificering i forhold til en gældende ISO/IEC 27001	5
2.3	Akkrediterede testvirksomheder	6
2.3.1	Krav til testvirksomhed	6
2.3.2	Krav til personale der udfører certificeringsarbejdet	6
2.3.3	Supervisering og signering af standardrapport	6
3.	Krav til ledelsessystem for informationssikkerhed	7
3.1	Personaleadministration	8
3.2	Kommunikations- og driftsstyring	8
3.2.1	Procedure og ansvar for drift	8
3.2.2	Planlægning og overvågning af ressourcer	8
3.2.3	Beskyttelse mod ondartet programkode	9
3.2.4	Backup	9
3.2.5	Netværkssikkerhed	9
3.2.6	Brug af offentlige netværk	9
3.2.7	Overvågning	10
3.2.8	Tidssynkronisering	10
3.3	Adgangskontrol	10
3.3.1	Fysisk adgangskontrol	10
3.3.2	Brugeradgang	10
3.3.3	Personleadgang	10
3.3.4	Adgangskontrol og sikkerhed i forhold til netværk	11
3.3.5	Adgangskontrol og sikkerhed i forhold til styresystemer	11
3.3.6	Adgangskontrol og sikkerhed i forhold til applikationer og information	11
3.4	Datavalidering mv.	11
3.4.1	Korrekt databehandling i applikationer	11
3.4.2	Sikring af krypteringsnøgler og digitale signaturer	11

Formålet med ledelses- system for informations- sikkerhed

1

Ledelsessystemet for informationssikkerhed skal sikre, at tilladelsesindehavers base platform og forretningsystem og spilleleverandørs spilplatform og forretningsystem beskyttes mod eventuelle trusler samt sikre de følsomme oplysninger systemerne indeholder. Ved at sikre integriteten og adgangen til platformene og forretningssystemernes varetages en række væsentlige sikkerhedshensyn i relation til tilladelsesindehaver og spilleleverandørs forretning, men også i forhold til beskyttelse af spillernes oplysninger og fortrolige oplysninger om tredjemænd.

1.1 Version

Version 1.0 af 2014.07.04

- Ny struktur i forhold til den tidligere version 1.3, samt en række opdateringer på en række områder. Derfor udstedes ny version 1.0. Det er hensigten fremover er at følge normal versioneringsnummerering.

Version 1.1 af 2015.12.21

- Udvidelse af anvendelsesområdet til også at omfatte udbud af lotterier og væddemål på heste- og hundevæddeløb.

Version 1.2 af 2020.01.01

- Spillemyndigheden har fjernet kravet om at testvirksomhedens akkreditering skal henvise til en specifik version jf. afsnit 2.3.

Version 2.0 af 2023.01.01

- Præcisering af hvilke testvirksomheder, der kan foretage en eventuel ISO 27001 certificering jf. afsnit 2.2. Opdatering af krav til akkrediterede testvirksomheder og personale. Derudover er der foretaget generelle tilpasninger og specificeringer.

Version 2.1 af 2023.10.01

- Opdateret visuelt layout af dokumentet. Få sproglige rettelser. Ingen ændringer til krav.

Version 3.0 af 2025.01.01

- Rettelser er foretaget i forhold til introduktion af tilladelser til spilleleverandører, hvilket betyder at begrebet spilsystem er ændret til begreberne 'base platform' og 'spilplatform'. Afsnittet om krav til supervisor er ændret.

Spillemyndigheden reviderer løbende certificeringsprogrammet for væddemål og onlinekasino. Den seneste version er tilgængelig på Spillemyndighedens hjemmeside.

Ved udgivelse af en ny version af certificeringsprogrammet offentliggør Spillemyndigheden, hvis nødvendigt, retningslinjer for en overgangsordning og gyldigheden af allerede gennemførte certificeringer.

Det skal fremhæves, at det er den danske version, der er bindende. Den engelske version er udelukkende af vejledende karakter.

1.2 Anvendelsesområde

Ledelsessystem for informationssikkerhed finder anvendelse på udbud af online væddemål (§ 11 i lov om spil), landbaseret væddemål (§ 11 i lov om spil), onlinekasino (§ 18 i lov om spil) og levering af spil (§ 24a i lov om spil).

Frekvens og testvirk- somheder

2

2.1 Certificeringsfrekvens

Tilladelsesindehaver og spilleleverandør er ansvarlig for at sikre, at der med et interval på maksimalt 12 kalendermåneder sker certificering i overensstemmelse med kravene i dette dokument.

2.1.1 Første certificering

Tilladelsesindehaver og spilleleverandør skal være certificeret første gang inden der kan udstedes tilladelse, medmindre Spillemyndigheden har oplyst andet. Se afsnit 2.1.3 i de generelle krav for yderligere oplysninger.

2.1.2 Fornyet certificering

Tilladelsesindehaver og spilleleverandør skal som udgangspunkt have foretaget en ny certificering inden 12 måneder fra seneste certificering. Det skal fremgå af standardrapporten, hvornår der er sket fornyet certificering.

Standardrapporten som dokumenterer den fornyede certificering skal være Spillemyndigheden i hænde senest to måneder efter, at certificeringen er foretaget.

2.1.3 Udsættelse af fornyet certificering

Tilladelsesindehaver og spilleleverandør kan udsætte certificeringen op til to måneder fra tidspunktet, hvor der skulle være foretaget en ny certificering. Den nye certificering skal således være afsluttet senest 14 måneder fra seneste certificering og standardrapporten skal være Spillemyndigheden i hænde inden samme frist.

Spillemyndigheden skal underrettes, inden certificeringen udsættes.

Fristen for fornyelse af certificering forkortes med den tid den tidligere 12 måneders frist har været udsat. Hvis man fx udnytter de maksimale to måneders udsættelse, skal næste certificering fornyes efter 10 måneder. Tidspunktet for næste certificering skal afspejle dette i standardrapporten.

2.2 Certificering i forhold til en gældende ISO/IEC 27001

Er tilladelsesindehaver eller spilleleverandør certificeret i forhold til en gældende ISO/IEC 27001, må det som udgangspunkt forventes, at tilladelsesindehavers eller spilleleverandørs ledelsessystem for informationssikkerhed er af en sådan kvalitet, at certificering i forhold til Spillemyndighedens ledelsessystem for informationssikkerhed SCP.03.00 er unødvendig.

Det er en forudsætning at certificering af ledelsessystemet for informationssikkerhed udføres som akkrediteret certificering af et certificeringsorgan, der er akkrediteret efter ISO/IEC 17021-1 til certificering i henhold til ISO/IEC 27001 af DANAK (Den Danske Akkrediteringsfond) eller et tilsvarende akkrediteringsorgan, som er medunderskriver af EA's (European cooperation for Accreditation) multilaterale aftale om gensidig anerkendelse mht. certificering af ledelsessystemer eller for certificeringsorganer udenfor EA's område af et akkrediteringsorgan, der er medunderskriver af den relevante multilaterale aftale om gensidig anerkendelse under IAF (International Accreditation Forum).

Det er en forudsætning, at det samlede scope for tilladelsesindehavers eller spilleleverandørers ISO/IEC 27001 certificering omfatter hele base platform eller spilplatform i dets fuldstændighed, som defineret i spillelovgivningen, og enhver arbejdsproces, der relaterer sig til platformene, samt alle geografiske placeringer af platformene.

For at kunne tage stilling til, hvorvidt ovenstående er opfyldt, skal den akkrediterede testvirksomhed have adgang til:

- Gældende ISO/IEC 27001 certificering,
- Statement of Applicability, og
- Risikovurderingen.

Op på denne baggrund kan den akkrediterede testvirksomhed så udstede certificering, der træder i stedet for en certificering i forhold til Spillemyndighedens ledelsessystem for informationssikkerhed SCP.03.00.DK.

2.3 Akkrediterede testvirksomheder

For at sikre, at de nødvendige kvalifikationer er til stede, når en certificering udføres, skal testvirksomheden og dennes ansatte leve op til kravene i dette afsnit.

2.3.1 Krav til testvirksomhed

Certificering af informationssikkerhedssystemet skal udføres som akkrediteret certificering af et certificeringsorgan, der er akkrediteret efter ISO/IEC 17021-1 eller ISO/IEC 17065 til certificering i henhold til Spillemyndighedens Certificeringsprogram SCP.03.00.DK af DANAK (Den Danske Akkrediteringsfond) eller et tilsvarende akkrediteringsorgan, som er medunderskriver af EA's (European co-operation for Accreditation) multilaterale aftale om gensidig anerkendelse mht. certificering af ledelsessystemer eller for certificeringsorganer udenfor EA's område af et akkrediteringsorgan, der er medunderskriver af den relevante multilaterale aftale om gensidig anerkendelse under IAF (International Accreditation Forum).

Dokumentation for testvirksomhedens akkreditering vedlægges certificeringsrapporten. Alternativt kan der linkes til akkrediteringen i certificeringsrapporten.

2.3.2 Krav til personale der udfører certificeringsarbejdet

Certificeringsarbejdet skal udføres af personale, der er tilstrækkeligt kvalificeret jf. kravene i afsnit 7 i ISO/IEC 17021-1 eller afsnit 6 i ISO/IEC 17065. Den akkrediterede testvirksomhed skal derfor ansætte og oplære tilstrækkeligt kvalificeret, kompetent og erfarent personale.

2.3.3 Supervisering og signering af standardrapport

Udførelsen af certificeringsarbejdet skal superviseres jf. kravene til supervisering i afsnit 2.3 i de generelle krav. Det er superviserens ansvar at underskrive standardrapporten og derved indestå for, at certificeringen er udført fagligt forsvarligt.

Krav til ledelsessystem for informationssikker- hed

3

Tilladelsesindehavers og spilleleverandørs informationssikkerhed afhænger i høj grad af at base platform, spilplatform, forretningssystemerne og forretningssystemgangene omkring dette er sikkert, og at uvedkommende ikke kan få adgang til oplysninger, de ikke er berettiget til.

Tilladelsesindehavers og spilleleverandør personale har en nøglerolle i forhold til adgangen til platformene. Derfor skal deres adgang til både base platform, spilplatform og forretningssystemet være klart defineret og aftalt i deres ansættelsesforhold med tilladelsesindehaveren eller spilleleverandøren. Dette skal bidrage til at begrænse uautoriseret adgang til base platform, spilplatform og forretningssystemet.

Teknisk set er der en række driftsmæssige tiltag, som tilladelsesindehaver og spilleleverandør skal implementere for at sikre base platformens, spilplatformens og forretningssystemets integritet. I forlængelse heraf er der krav til anvendelsen af sikre kommunikationskanaler. Informationssikkerhed skal også tænkes ind i den måde, som base platform, spilplatform og forretningssystemet udvikles på, så data ikke forvansktes som følge af manglende validering af datainput fra applikationer.

Tredjemænd kan også have adgang til base platform, spilplatform, forretningssystemerne eller ledelsessystemet omkring disse, hvis de fx er underleverandører eller indtager en anden position i tilladelsesindehavers eller spilleleverandørs virksomhed, som kræver adgang til base platform, spilplatform, forretningssystemet eller ledelsessystemet.

Uanset hvem der har adgang til base platform, spilplatform og forretningssystemet, skal denne adgang være tilpasset den enkelte person, så personer ikke kan tilgå information, der er uvedkommende for det arbejde, de udfører.

3.1 Personleadministration

Tilladelsesindehaver og spilleleverandør skal have en politik for oprettelse, ændring og afvikling af personalets brugeradgang til base platform, spilplatform og forretningssystemerne. På baggrund af politikken skal der udarbejdes en formel procedure, der sikrer:

- at der foreligger en detaljeret arbejdsbeskrivelse for den enkelte medarbejder,
- at der gives brugeradgang til base platform, spilplatform og forretningssystemet i overensstemmelse med medarbejderens arbejdsbeskrivelse,
- at brugeradgangen ændres i overensstemmelse med en ændret arbejdsbeskrivelse, og
- at brugeradgangen afvikles i forbindelse med medarbejderens ansættelses ophør.

Tilsvarende politikker og procedure skal foreligge for konsulenters og/eller andre tredjemænds bruger-adgang til base platform, spilplatform og forretningssystemet, hvis sådanne tildeles adgang.

3.2 Kommunikations- og driftsstyring

3.2.1 Procedure og ansvar for drift

Base platformen, spilplatformen og forretningssystemerne skal kunne lukke hensigtsmæssigt ned i tilfælde af strømafbrydelse. Nødstrøm er derfor påkrævet for at sikre dataintegritet, logs, backup og for at sikre, at igangværende spil kan afvikles og afsluttes.

3.2.2 Planlægning og overvågning af ressourcer

Base platform, spilplatform og forretningssystemerne skal føre en log over systemets ydeevne og på baggrund heraf kunne danne rapporter.

Systemernes ressourceforbrug skal overvåges og tilpasses, og der skal laves prognoser for kravene til den fremtidige kapacitet for at sikre den nødvendige ydelse.

3.2.3 Beskyttelse mod ondartet programkode

Base platform, spilplatform og forretningssystemerne skal have redskaber til at opdage og forhindre indtrængning og indsættelse af uautoriseret programkode.

3.2.4 Backup

Base platform, spilplatform og forretningssystemerne skal lave backup af alle driftskritiske data og skal kunne genskabe alle driftskritiske data fra backup.

Base platform, spilplatform og forretningssystemerne skal være i stand til at genskabe alle kritiske data, der er genereret i perioden fra tidspunktet for den seneste backup til tidspunktet, hvor et systemnedbrud fandt sted eller en systemfejl opstod.

3.2.5 Netværkssikkerhed

Base platform, spilplatform og forretningssystemerne skal indrettes så enheder i samme broadcast-domæne(r) ikke kan skabe netværksadgang uden om firewallen.

Udstyr, der anvendes som firewall, skal være dedikeret til firewallfunktionen og kun indeholde firewall-relaterede brugerkonti og funktioner.

Adgang til firewallen skal begrænses til arbejdsstationer, der indgår i konfigurationsudgangspunktet, som defineret i Spillemyndighedens program for styring af systemændringer SCP.06.00.DK og skal afvise alle datapakker, der kommer fra andre steder end arbejdsstationer, der indgår i konfigurationsudgangspunktet.

Firewallen skal vedligeholde en revisionsegnet log med alle systemændringer, der påvirker forbindelses-tilladelserne, og alle succesfulde og mislykkedes forsøg på at få adgang til den.

3.2.6 Brug af offentlige netværk

Anvender tilladelsesindehaver eller spilleleverandør offentlige netværk til datatrafik mellem geografisk spredte del-systemer, skal informationen være krypteret og del-systemerne anvende autentifikation.

Al kommunikation mellem geografisk spredte del-systemer skal beskytte mod:

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

Tilladelsesindehaver og spilleleverandør skal anvende en sikker primær DNS og en sikker sekundær DNS, der er logisk og fysisk adskilt fra den primære DNS.

3.2.7 Overvågning

Base platform, spilplatform og forretningssystemerne skal føre revisionsegneede logge, der registrerer:

- brugeraktivitet,
- undtagelser (exceptions), og
- informationssikkerhedshændelser.

De revisionsegneede logge skal gemmes i mindst 5 år og skal beskyttes mod uautoriseret adgang.

Base platform, spilplatform og forretningssystemerne skal registrere alle fejl og nedbrud samt løbende overvåge anvendelsen og funktionsdygtigheden af væsentlige systemkomponenter. Væsentligheden følger af klassificeringen af komponenter i Spillemyndighedens program for styring af systemændringer SCP.06.00.DK.

3.2.8 Tidssynkronisering

Der skal ske tidssynkronisering med en autoritativ tidsserver på base platform, spilplatform og forretningssystemerne med et passende interval, for at sikre ensartethed i det tidsstempel, der eksempelvis anvendes i forbindelse med registrering i logs.

3.3 Adgangskontrol

Tilladelsesindehaver og spilleleverandør skal have adgangskontrol til at beskytte systemernes hardware, samt brugeradgangen til systemerne.

3.3.1 Fysisk adgangskontrol

Der skal være fysisk adgangskontrol til adgangen til den hardware hvorpå base platform, spilplatform og forretningssystem afvikles, samt øvrigt udstyr hvorfra man kan tilgå systemer.

Niveauet af adgangskontrol skal tilpasses væsentligheden af de systemer man kan tilgå fra det pågældende udstyr.

3.3.2 Brugeradgang

Base platform, spilplatform og forretningssystemerne skal kræve stærke kodeord i forbindelse med brugeradgang til systemet, og pauseskærm skal aktiveres eller automatisk logge brugeren af systemet ved længere tids inaktivitet.

3.3.3 Personleadgang

Muligheden for at give adgang til base platform, spilplatform og forretningssystemerne skal være begrænset til så få medarbejdere som muligt, og både base platform, spilplatform og forretningssystemerne skal kunne understøtte differentieret brugeradgang, så politikken og proceduren for personaleadministration, jf. afsnit 3.1, kan udmøntes i praksis.

Førstegangskodeordet skal skiftes til et kodeord valgt af brugeren ved første login.

3.3.4 Adgangskontrol og sikkerhed i forhold til netværk

Der skal være adgangskontrol til base platform, spilplatform og forretningssystemernes netværksfunktioner, og bruger-adgang hertil må kun kunne opnås gennem denne adgangskontrol. Base platform, spilplatform og forretningssystemet skal forhindre uautoriseret intern og ekstern adgang til netværksfunktioner.

Base platform, spilplatform og forretningssystemernes skal benytte segregerede netværk, så grupper af relaterede funktioner, brugere og del-systemer kan holdes adskilt fra hinanden.

3.3.5 Adgangskontrol og sikkerhed i forhold til styresystemer

Alle brugere skal have et unikt brugernavn/ID, som kun er til personligt brug, og base platform, spilplatform og forretningssystemerne skal anvende passende autentifikationsmetoder til at sikre brugerens identitet ved log ind.

Netværkstrafikstyring skal benyttes til at kontrollere adgangen til styresystemet på væsentlige systemkomponenter. Væsentligheden følger af klassificeringen af komponenter i Spillemyndighedens program for styring af systemændringer SCP.06.00.DK.

Når et styresystem installeres på udstyr, der er en del af base platformen eller spilplatformen, må der kun installeres/aktiveres funktioner, der er strengt nødvendige for, at udstyret kan opfylde sit formål. Programmer og lignende, der kan tilsidesætte adgangskontrollen, må under ingen omstændigheder installeres på base platform, spilplatform og forretningssystemerne.

3.3.6 Adgangskontrol og sikkerhed i forhold til applikationer og information

Alle brugere skal have et unikt brugernavn/ID, som kun er til personligt brug, og base platform, spilplatform og forretningssystemerne skal anvende passende autentifikationsmetoder til at sikre brugerens identitet ved log ind.

Følsom information skal gemmes og sendes i krypteret form, og base platform, spilplatform og forretningssystemerne skal sikre en særlig streng adgangskontrol for brugeres adgang til disse.

3.4 Datavalidering mv.

3.4.1 Korrekt databehandling i applikationer

Datainput til applikationer skal valideres for at sikre, at datainput er passende i den pågældende kontekst og ikke er skadelig for base platform, spilplatform og forretningssystemerne.

Løbende automatisk datavalidering skal indarbejdes i alle applikationer for at sikre mod dataforvanskning og driftsforstyrrelser.

Dataoutput fra applikationer skal valideres for at sikre, at behandlingen af den gemte information er foregået korrekt.

3.4.2 Sikring af krypteringsnøgler og digitale signaturer

Krypteringsnøgler, digitale signaturer og lignende skal opbevares sikkert.

