

Spillemyndighedens program for styring af systemændringer

Version 1.1.0 af 1. september 2011

Indhold

1 Indledning.....	3
1.1 Myndighed.....	3
1.2 Formål.....	3
1.3 Målgruppe	3
1.4 Version.....	3
1.5 Henvendelser.....	3
2. Rammen for styring af systemændringer.....	4
2.1 Ansvar ved håndtering af ændringer.....	4
2.1.1 Tilladelsesindehavers ansvar	4
2.1.2 Ansvarlig for styring af systemændringer	4
3. Forløb for ændringer	5
3.1 Planlægning af ændringer	5
3.2 Identifikation af konfiguration.....	5
3.3 Systemstruktur og valg af konfigurationselementer.....	5
3.4 Identifikation af komponenter ("assets").....	6
3.5 Information om konfigurationselementer	6
3.6 Geografisk placering af komponenter	6
3.7 Inddeling af komponenter	6
3.8 Konfigurationsudgangspunktet	7
4. Styring af systemændringer.....	7
4.1 Begrundelse for systemændringer	7
4.2 Evaluering af systemændringer.....	8
4.3 Godkendelse af systemændringer.....	8
4.3.1 Afviste ændringer, anbefalet af leverandører af forretningsfunktioner.....	9
4.3.2 Godkendte ændringer, anbefalet af leverandører af forretningsfunktioner	9
4.3.3. Afviste ændringer, anbefalet af leverandører af spilfunktioner	9
4.3.4 Godkendte ændringer, anbefalet af leverandører af spilfunktioner	9
4.3.5 Random Number Generator (RNG) og nye spil	9
4.4 Implementering og verifikation af systemændringer.....	9
4.5 Redegørelse for status af systemændringer	10
4.6 Indberetninger.....	10
4.7 Ændrings- og konfigurationsrevision.....	11

1 Indledning

1.1 Myndighed

Dette dokument "Spillemyndighedens program for styring af systemændringer" er udstedt af Spillemyndigheden i henhold til spilleloven (nr. 848 af 1.juli 2010 med senere ændringer) og bekendtgørelserne om onlinekasino, online væddemål og landbaserede væddemål, og er en del af det samlede certificeringsprogram, som består af dokumenterne "Spillemyndighedens krav til akkrediterede testvirksomheder", "Spillemyndighedens program for styring af systemændringer" og "Spillemyndighedens tekniske standarder".

1.2 Formål

Dokumentet fastsætter de minimumskrav, som en tilladelsesindehaver skal efterleve, når de foretager ændringer i deres spilsystem.

1.3 Målgruppe

Dokumentet er rettet mod tilladelsesindehaver, leverandører, akkrediteringsorganer og testvirksomheder.

1.4 Version

Dette dokument er version 1.1.0 af 1. september 2011.

Spillemyndigheden vil løbende revidere certificeringsprogrammet og seneste version samt versionshistorik er tilgængelig på spillemyndighedens hjemmeside: <http://spillemyndigheden.dk>.

Ved ændringer i certificeringsprogrammet vil certificeringer som udgangspunkt fortsat være gyldige i den periode, de er udstedt for.

Det skal fremhæves, at det er den danske version, der er bindende og den engelske version udelukkende stilles til rådighed som vejledning.

1.5 Henvendelser

Alle henvendelser, der vedrører dette dokument, bør stilles skriftligt til denne adresse:

spillemyndigheden@skat.dk

eller

Spillemyndigheden
Helgeshøj Allé 9
2630 Taastrup

2. Rammen for styring af systemændringer

Tilladelsesindehaver skal tilrettelægge sin interne procedure for styring af ændringer, således at de enkelte ændringer og virkningen af ændringerne på det samlede system til enhver tid kan identificeres.

En del af den interne procedure er, at tilladelsesindehaver skal have en ansvarlig for styring af systemændringer, jf. afsnit 2.1.2, der skal sikre, at der udarbejdes en formel ændringsplan, der beskriver alle de specifikke procedurer og at de forskellige tiltag er samordnet.

Programmet for styring af systemændringer er opbygget således, at rutineændringer mv., kan gennemføres på en hensigtsmæssig og kontrolleret måde, samtidig med at det får minimal indflydelse på tilladelsesindehavers forretningsgang.

Tilladelsesindehaver skal sikre, at der sker en certificering efter "Spillemyndighedens program for styring af systemændringer", og denne skal være gennemført, inden tilladelsesindehavers udbud af væddemål og onlinekasino finder sted.

Certificeringen udstedes med en gyldighed af 12 måneder.

2.1 Ansvar ved håndtering af ændringer

2.1.1 Tilladelsesindehavers ansvar

Tilladelsesindehaver er ansvarlig for ændringer i deres systemer vedrørende væddemål og onlinekasino, uanset om disse ændringer er gennemført af tilladelsesindehaveren, en leverandør eller en tjenesteudbyder.

Tilladelsesindehaveren til væddemål og onlinekasinospil skal klarlægge og beskrive ansvar og beføjelser i forbindelse med gennemførelse og godkendelse af ændringsforløbet. Hvis systemændringerne er styret af en af tilladelsesindehaverens leverandører, skal tilladelsesindehaveren sørge for, at leverandøren gennemfører tilsvarende procedurer, og at denne overholder kravene i dette dokument.

2.1.2 Ansvarlig for styring af systemændringer

Tilladelsesindehaver skal udpege én eller flere ansatte i virksomheden, der er overordnet ansvarlig for systemændringer. Det kan tilrettelægges som et udvalg.

Den eller de ansvarlige personer skal have tilstrækkeligt erfaring og kompetence samt være højt placeret i virksomheden.

Den eller de ansvarlige personer skal ikke nødvendigvis selv varetage systemændringerne, idet disse vil variere meget alt efter hvad der er relevant i forhold til den enkelte ændring. Det skal være i samarbejde med andre medarbejdere i virksomheden/leverandører, så der kan tages kvalificerede beslutninger på alle områder. Der skal føres en log over, hvem der har deltaget i beslutningsprocessen.

Forud for godkendelse af ændringer, skal den eller de ansvarlige personer bekræfte, at:

- de foreslåede systemændringer er i overensstemmelse med "Spillemyndighedens tekniske standarder"
- de foreslåede systemændringer er nødvendige,

- konsekvenserne vil være acceptable,
- systemændringerne er nøje overvejet, dokumenteret og kategoriseret og
- de planlagte handlinger for gennemførelsen af systemændringerne i dokumenter, hardware og/eller software er tilfredsstillende.

3. Forløb for ændringer

3.1 Planlægning af ændringer

Den formelle ændringsplan skal indeholde en beskrivelse af, at systemændringerne

- inkorporeres og integreres med leverandørens ændringsplaner,
- skal være dokumenteret og godkendt af direktionen,
- skal være kontrolleret af den eller de ansvarlige personer,
- skal vise hvilken konfiguration, der skal bruges,
- skal referere til tilladelsesindehavers og leverandørens relevante procedurer, når det er muligt og
- skal fastsætte, hvem der er ansvarlige for ændringer gennem systemet og komponenternes livscyklus, og med hvilke beføjelser.

3.2 Identifikation af konfiguration

Konfigurationen, der er beskrevet nedenfor, er et minimumskrav. Formålet er at gøre en identifikation af alle de forskellige dele i systemkonfigurationen mulig, så systemændringernes betydning for alle dele bliver vurderet i sammenhæng med dette dokumentets formål.

3.3 Systemstruktur og valg af konfigurationselementer.

Valget af konfigurationselementer og deres indbyrdes forbindelser bør beskrive systemstrukturen. Konfigurationselementer bør vælges ud fra, om deres funktionelle og fysiske egenskaber kan håndteres separat.

Udvælgelseskriterierne bør omhandle:

- krav i lovgivningen,
- kritiske i forhold til sikkerhedsrisiko (risiko i forhold til fortrolighed, integritet og tilgængelighed) og ansvarlighed,
- ny eller ændret teknologi, design eller udvikling og
- grænseflade til andre konfigurationselementer.

Antallet af de valgte konfigurationselementer bør optimere muligheden for at kontrollere produktet. Udvælgelsen af konfigurationselementer bør igangsættes så hurtigt som muligt i produktets livscyklus. Konfigurationselementer bør vurderes løbende i takt med, at produktet udvikles.

Ethvert konfigurationselement, der kan have indflydelse på fortroligheden, integriteten eller ansvarlighed, bør vurderes ud fra ovennævnte kriterier.

3.4 Identifikation af komponenter ("assets")

Tilladelsesindehaver skal sammen med sine leverandører kortlægge alle hardware- og softwarekomponenter, der indgår i driften af væddemål og onlinekasino. Komponenter, der kan have indflydelse på sikkerheden (integritet, fortrolighed og tilgængelighed) og/eller er ansvarlige for betaling eller for spilsystemer, skal indarbejdes i et register over komponenter.

Detaljeringsgraden af dette register vil være op til tilladelsesindehaver og dennes leverandører. Hvis en tilladelsesindehaver vælger at føre et generelt register (fx "spilsystemet" er eneste komponent) vil enhver ændring i spilsystemet blive klassificeret som en ændring til et væsentligt konfigurationselement og dermed underlagt passende kontrol. Hvis detaljeringsgraden i registret derimod er større (fx software RNG.klasse), vil ændringer i mindre vigtige konfigurationselementer kunne håndteres ved mindre gennemgribende tiltag.

Elementerne skal have en unik kode, versionsnummer og identifikationskarakteristik, således at en uafhængig kontrollant har mulighed for at inspicere/kontrollere nogle eller alle dele på et hvilket som helst tidspunkt og afgøre, om det har ændret sig fra udgangspunktet.

Elementerne skal oprettes i registret over komponenter. Der bør som udgangspunkt identificeres en ejer af hver komponent. Ejeren skal være den ansvarlige for ændringer af komponenterne. Kan en sådan ejer ikke identificeres, er det den eller de ansvarlige personer, jf. afsnit 2.1.2, der er ansvarlig for komponenten.

Registret over komponenter skal sammen med loggen over ændringer være det udgangspunkt, der identificerer spilsystemet.

3.5 Information om konfigurationselementer

Information om konfigurationselementer indeholder både en definition af elementet og information om driften af produktet, der entydigt identificerer et element, så en kontrollant kan vurdere, om den er i overensstemmelse med planen (fx kontrolsum for kilde, objekt og eksekverbar kode). Information om konfigurationselementer med "væsentlig relevans", jf. afsnit 3.7, skal inkluderes, eller henvises til, i registret over komponenter.

Information om konfigurationen bør være relevant og sporbar. Nummereringen skal være unik og sikre en behørig kontrol med det pågældende konfigurationselement.

3.6 Geografisk placering af komponenter

Den geografiske placering af alle servere og hardware-komponenter skal fremgå af registret over komponenter.

3.7 Inddeling af komponenter

Alle elementer, der er identificeret i registret for komponenter, skal klassificeres ud fra følgende matrix:

Fortrolighed henviser til fortrolige oplysninger om kunder.

Integritet henviser til integriteten af systemernes funktionalitet og den information, systemerne indeholder.

Tilgængelighed henviser til tilgængeligheden af den information, der drejer sig om kundeforpligtigelser.

Ansvarlighed henviser til alle brugernes aktivitet (kunder, ansatte, tredjepart) på alle komponenterne i systemet.

Alle komponenter skal have en relevanskode på en skala fra 1-3 baseret på konfigurationselementernes relevans i forhold til at skabe eller beskytte alle systemets egenskaber (fortrolighed, integritet, tilgængelighed eller ansvarlighed).

Relevanskoderne er:

1 = ingen relevans (kan ikke have nogen negativ indflydelse på systemets egenskaber),

2 = nogen relevans (kan have indflydelse på systemets egenskaber) og

3 = væsentlig relevans (systemegenskaber er konkret relateret til konfigurationselementet).

Når komponenterne skal klassificeres, kan det være relevant at vurdere den materielle forskel mellem væddemål og onlinekasino, og de forskellige risici, der er forbundet hermed (inklusive kundeforpligtigelser og fairness).

3.8 Konfigurationsudgangspunktet

Konfigurationsudgangspunktet består af oplysninger om konfigurationen, der giver en definition af produktet, der er godkendt af en akkrediteret testvirksomhed. Konfigurationsudgangspunktet, samt godkendte ændringer til denne, danner grundlag for det nye konfigurationsudgangspunkt.

Konfigurationsudgangspunktet skal godkendes hvert år af en akkrediteret testvirksomhed.

4. Styring af systemændringer

Omfanget af den enkelte systemændring vil påvirke graden af den styring, der er nødvendig for at håndtere en foreslået systemændring.

Forløbet for styring af systemændringer skal dokumenteres, og denne dokumentation skal indeholde følgende:

- en beskrivelse af, en begrundelse for og en registrering af ændringerne,
- en kategorisering af ændringerne, hvad angår kompleksitet, ressourcer og planlægning,
- en evaluering af de konsekvenser, ændringerne har,
- detaljer om, hvordan ændringerne skal godkendes og
- detaljer om, hvordan ændringerne skal gennemføres og efterprøves

4.1 Begrundelse for systemændringer

Forud for den interne godkendelse af systemændringer af den eller de ansvarlige personer skal alle ændringsforslag identificeres og dokumenteres.

Forslag til systemændringer bør typisk indeholde følgende oplysninger:

- konfigurationselement(er) og relaterede oplysninger, der skal ændres, inklusiv detaljer om deres benævnelse og nuværende revideringsstatus,
- en beskrivelse af den foreslåede ændring,
- detaljer om andre konfigurationselementer eller oplysninger, der kan blive påvirket af ændringerne,
- den medarbejder/leverandør, der har udarbejdet forslaget og datoen for udarbejdelsen,
- årsag til ændringen og
- ændringstype.

Status for ændringsforløbet, relaterede beslutninger og dispositioner skal dokumenteres. En typisk metode til at dokumentere ændringer er at bruge en blanket, der har et unikt identifikationsnummer for at lette identifikationen og sporbarheden af blanketten.

Udgangspunktet for ændringer, anbefalet af leverandører af forretningsfunktioner, bør være, at ændringerne er begrundet og berettiget.

4.2 Evaluering af systemændringer

Evaluering af de foreslåede systemændringer skal udføres og dokumenteres. Denne evaluering skal indeholde:

- tekniske fordele ved de foreslåede ændringer,
- risici ved ændringerne,
- indflydelse på efterlevelsen af lovgivningen,
- fortrolighed af kundedata,
- integriteten af funktionalitet og data,
- tilgængelighed af kundedata og midler og
- ansvarlighed ved brugersamspil med systemet.

Selvom ændringer, anbefalet af leverandører af forretningsfunktioner, generelt vil blive opfattet som begrundet og berettiget, bør tilladelsesindehavere stadig evaluere sådanne ændringer ud fra kriterierne ovenfor.

4.3 Godkendelse af systemændringer

Der skal etableres et forløb for den formelle godkendelse af systemændringerne.

Efter en foreslået ændring er blevet evalueret, skal den eller de ansvarlige personer bedømme evalueringen og beslutte, om ændringen skal godkendes eller ej.

Selv om ændringer, anbefalet af leverandører af forretningsfunktioner, generelt bliver opfattet som begrundet og berettiget, bør tilladelsesindehavere stadig formelt godkende eller afvise sådanne ændringer.

Alle overvejelser og beslutninger om systemændringer bør noteres i en log. Varsling af beslutninger bør cirkuleres til de relevante interessenter inden for og uden for organisationen, inklusiv den relevante akkrediterede testvirksomhed.

Den akkrediterede testvirksomhed skal analysere grundlaget for alle beslutninger, der afviger fra anbefalingerne fra leverandørerne. Alle beslutninger skal håndteres separat. Den akkrediterede testvirksomhed skal attestere, om tilladelsesindehaverens beslutning er berettiget.

4.3.1 Afviste ændringer, anbefalet af leverandører af forretningsfunktioner

Når tilladelsesindehaveren beslutter ikke at følge en anbefaling fra en leverandør, skal beslutningen begrundes.

Begrundelsen for ikke at følge leverandørens anbefalinger skal gives til Spillemyndigheden gennem den akkrediterede testvirksomhed hvert kvartal.

Den akkrediterede testvirksomhed skal analysere grundlaget for hver enkelt beslutning om ikke at følge leverandørens anbefalinger separat. Den akkrediterede testvirksomhed skal vise, om tilladelsesindehaverens beslutning er berettiget.

4.3.2 Godkendte ændringer, anbefalet af leverandører af forretningsfunktioner

Når en tilladelsesindehaver beslutter, at det er hensigtsmæssigt at følge anbefalingerne fra en leverandør, skal dette gøres så komponenterne beskrevet i register for komponenter, jf. afsnit 3.4, ikke udsættes for unødvendige risici.

Tiden mellem leverandørens anbefalinger og implementering skal begrundes i en log. Dokumentation for implementering af leverandørens anbefalinger skal fremgå af den samme log. Denne log skal efterfølgende overdrages til den akkrediterede testvirksomhed og Spillemyndigheden årligt.

4.3.3. Afviste ændringer, anbefalet af leverandører af spilfunktioner

Når tilladelsesindehaveren beslutter, at det ikke er hensigtsmæssigt at følge de anbefalinger, som leverandør af spilfunktioner har udsendt, skal den pågældende tilladelsesindehaver begrunde dette. Den dokumenterede begrundelse skal indeholde vurdering for komponenterne, der er beskrevet i register for komponenter, jf. afsnit 3.4, vil kunne ske.

Begrundelsen for ikke at følge leverandørens anbefalinger skal gives til Spillemyndigheden gennem den akkrediterede testvirksomhed hvert kvartal.

Den akkrediterede testvirksomhed skal analysere grundlaget for hver enkelt beslutning om ikke at følge leverandørens anbefalinger separat. Den akkrediterede testvirksomhed skal vise, om tilladelsesindehaverens beslutning er berettiget.

4.3.4 Godkendte ændringer, anbefalet af leverandører af spilfunktioner

Når en tilladelsesindehaver beslutter, at det er hensigtsmæssigt at følge anbefalingerne fra en leverandør, skal dette gøres så komponenterne beskrevet i register for komponenter, jf. afsnit 3.4, ikke udsættes for unødvendige risici.

Tiden mellem leverandørens anbefalinger og implementering skal begrundes i en log. Dokumentation for implementering af leverandørens anbefalinger skal fremgå af den samme log. Denne log skal efterfølgende overdrages til den akkrediterede testvirksomhed og Spillemyndigheden årligt.

4.3.5 Random Number Generator (RNG) og nye spil

Alle ændringer i RNG og implementering af helt nye spil skal godkendes af Spillemyndigheden før implementeringen finder sted.

4.4 Implementering og verifikation af systemændringer

Dette afsnit gælder for ændringer af komponenter (assets) klassificeret som 2 og 3 på baggrund af afsnit 3.7.

Efter gennemførelse skal overensstemmelse med de godkendte ændringer verificeres. Denne verificering skal registreres for at gøre den sporbar.

Gennemførte ændringer skal rapporteres til den relevante akkrediterede testvirksomhed (bemærk at for ændringer med lav risiko, kan dette ske ved at lave en rutinemæssig log over ændringer).

Den relevante akkrediterede testvirksomhed skal analysere risikoen ved alle ændringer til komponenterne i spilsystemet, der er rangeret 3 ("væsentlig relevans") som beskrevet i afsnit 3.7 og certificere alle ændringer, hver gang der sker ændringer.

Den relevante akkrediterede testvirksomhed skal analysere risikoen ved alle ændringer til spilfunktioner og certificere disse hvert kvartal.

Den relevante akkrediterede testvirksomhed skal analysere risikoen ved alle ændringer til forretningsfunktioner og certificere disse hvert år.

Vejledning til akkrediterede testvirksomhed: Analysen af risikoen ved ændringer bør laves med udgangspunkt i en forsvarlig stikprøvemetode og stå mål med den vurderede relevans af og risiko ved ændringen. Således at en komplet revision af alle ændringer ikke nødvendig.

Alle certificeringer udfærdiget af akkrediterede testvirksomheder skal fremsendes til Spillemyndigheden.

4.5 Redegørelse for status af systemændringer

Redegørelsen for status af systemændringer relaterer sig til spilsystemet og konfigurationsinformation.

Tilladelsesindehaveren skal sikre, at konfigurationsstatus bliver registreret løbende, og at denne viser status for konfigurationen af spilsystemet. Loggen for status af konfiguration bør indeholde:

- oplysning om systemopsætning (så som identifikationsnummer, titel, ikrafttrædelsesdatoer, status for revision, ændringshistorik og dens indtræden i udgangspunktet for konfigurationen),
- konfigurationen af systemer og komponenter (så som delnummer, produktdesign eller versionsstatus),
- status for udgivelsen af nye produktkonfigurationsoplysninger,
- risikoanalyse og beslutninger, der vedrører beslutningen om ændringerne bliver godkendt eller ej,
- implementering og
- certificering (se "Spillemyndighedens krav til akkrediterede testvirksomheder").

Oplysninger om konfigurationen og systemets evolution skal noteres på en måde, der fastlægger krydshenvisninger og de forbindelser, der er nødvendige for at give de nødvendige indberetninger jf. afsnit 4.6.

Redegørelse for status af ændringer skal sikre, at en detaljeret revision kan følge revisionssporet gennem ændringerne og klarlægge hvor ændringerne fandt sted, og hvem, der var ansvarlig for gennemførelsen af opsætningsændringerne (inklusiv men ikke begrænset til kildekode).

Detaljeringsgraden af redegørelsen for ændringerne bør være proportionelt med klassifikationen (1-3), jf. afsnit 3.7.

4.6 Indberetninger

Forskellige typer af indberetninger er nødvendige for håndtering af ændringer og konfigurationen. Disse indberetninger kan dække over enkelte konfigurationselementer eller hele systemet.

Typiske indberetninger indeholder:

- en liste med oplysninger om konfiguration af produkt, der er med i et specifikt konfigurationsudgangspunkt

- en liste med konfigurationselementer og deres konfigurationsudgangspunkt
- detaljer om den nuværende status for revision og ændringshistorik
- statusindberetninger om ændringer og afvigelser og
- detaljer om status for leverede og vedligeholdte systemkomponenter, herunder serienummer eller lignende samt revisionsstatus.

4.7 Ændrings- og konfigurationsrevision

Revision af ændringer og konfiguration skal udføres hvert år af en akkrediterede testvirksomhed.

Formålet ved den årlige revision af ændringer og konfiguration, er, at bekræfte, at program for styring af systemændringer er fulgt i løbet af året, og at logbogen korrekt viser status for systemet og ændringer.