LISEBERG

IT-säkerhetsdirektiv

Antaget den 30 juni december 2016 av styrelsen för Liseberg

1. Bakgrund

Detta IT-säkerhetsdirektiv har utarbetats av Liseberg och skall utgöra ett komplement till det IT-direktiv som vid var tid är gällande för Liseberg.

IT-säkerhetsarbetet inom Liseberg skall säkra att gäster, samarbetspartners och den egna verksamheten inte skadas eller utsätts för onödig risk orsakad av bristande IT-säkerhetsarbete.

IT-säkerhetsarbetet syftar till att:

- minimera sårbarheten
- säkra högsta möjliga tillgänglighet för systemanvändare
- säkra informationskvalitén

2. Information och ansvar

Det är upp till varje chef att ansvara för att detta direktiv ~~sprids och~~ efterlevs bland medarbetarna, det är också varje chefs ansvar att vidta åtgärder mot brott mot detta direktiv.

Varje anställd har ett personligt ansvar att informera sig om de regelverk, rutiner och det ansvar som är tillämpliga.

3. Anställdas skyldighet att efterfölja bestämmelserna i detta direktiv

Varje anställd är skyldig att följa detta direktiv och de säkerhets- och andra anvisningar som omfattas av den. Problem och överträdelser av dessa anvisningar bör rapporteras till närmsta chef eller till personuppgiftsombudet.

Liseberg skall löpande informera och utbilda all berörd personal om IT-säkerhet samt regelbundet genomföra tester av IT-säkerheten.

Detta direktiv och tillhörande anvisningar finns tillgänglig för alla anställda på Lisebergs Intranät tillsammans med Lisebergs IT-direktiv och skall löpande kommuniceras till samtliga anställda med tillgång till Lisebergs IT-system.

Antaget den 30 juni december 2016 av styrelsen för Liseberg

4. Huvudprinciper

All användning av Lisebergs IT-system skall ske i enlighet med Lisebergs IT-direktiv och detta IT-säkerhetsdirektiv.

Lisebergs IT-system är till för att stödja Lisebergs verksamhet och användare har därför inte rätt att utnyttja dessa i strid med Lisebergs affärsintressen eller på ett sätt som kan skada Lisebergs anseende.

All information som finns lagrad i Lisebergs IT-system är konfidentiell, därför har varje användare ansvar för att hantera sådan utrustning som har tilldelats honom/henne så, att utrustningen och i denna lagrad information inte kan missbrukas eller bli tillgänglig för utomstående.

Varje användare har ansvar för sitt personliga användar-ID och därtill hörande lösenord och för att dessa inte kan missbrukas. Lösenordet bör utformas och hanteras enligt de säkerhetsanvisningar som utarbetas av Lisebergs IT-avdelning.

Ingen utrustning får kopplas in mot Lisebergs IT-system utan tillstånd från Lisebergs IT-avdelning.

Ingen mjukvara utom den som tillhandahålls av Lisebergs IT-avdelning får installeras på sådan utrustning som har tilldelats användare.

5. Granskning och revidering

Syftet med detta dokument är att beskriva de regler och rutiner som gäller för säkerheten avseende både person, information och egendom vid Liseberg.

Även om detta IT-säkerhetsdirektiv är avsett att vara ett styrande dokument med lång giltighetstid så kan den påverkas av såväl organisatoriska som tekniska förändringar och förändrade myndighetskrav. Liseberg avser således att regelbundet utvärdera och uppdatera detta IT-säkerhetsdirektiv utifrån förändringar av den hotbild som finns för Lisebergs IT-system samt upprätta adekvata regler och rutiner för uppföljning och efterlevnad av direktivet.

Liseberg är skyldig att informera samtliga användare om förändringar i direktivet eller därtill hörande anvisningar.

6. Skydd av utrustning

När en anställd lämnar sin arbetsplats, konferensrum (även bara temporärt) eller till exempel tar emot besökande finns det risk att obehöriga tar del av information som finns på exempelvis datorskärmen, i skrivare och på skrivbordet.

Antaget den 30 juni december 2016 av styrelsen för Liseberg

För att minska risken för obehörig åtkomst av sådan information skall datorskärmen vara blank, alternativt skärmsläckare med lösenord aktiverad, inga papper av konfidentiell art lämnade i skrivare samt skrivbordet vara städat från säkerhetsklassad information och flyttbara datamedia.

Datorer som är belägna i utrymmen där obehöriga personer i form av kunder, besökare och andra, vistas skall ha bildskärmen vänd så att sådana personer inte kan läsa informationen. I möjligaste mån skall datorer i utrymmen där besökande vistas vara placerade bakom disk.

6.1. Regler för skydd

Regler som skall tillämpas är:

- Användaridentitet och lösenord får ej antecknas där andra kan få tillgång till uppgifterna.
- Personlig inloggningsinformation får aldrig överlåtas eller delges någon annan person.
- Alltid logga ut alternativt lås datorn när datorn lämnas utan uppsikt.
- Persondatorer skall inte lämnas påloggade efter arbetstid.
- Sekretessbelagd eller annat känsligt eller kritiskt material skall, när det inte används, förvaras på säkert sätt.
- Information skall ej delas med någon utan att vara säker på att sådan person är behörig att ta del av informationen.
- Känslig eller sekretessbelagd information ska skrivas ut på en skrivare som användaren har uppsikt över och till vilken obehöriga ej har eller enkelt kan skaffa sig tillgång till.

Liseberg är i det dagliga arbetet beroende av funktionaliteten i IT-systemen. Det är därför utomordentligt viktigt att Lisebergs IT-miljö skyddas från skadliga program som t.ex. virus men även andra former av skadliga program.

För att skydda Lisebergs IT-system skall därför dessa omgärdas av en heltäckande, aktiv och uppdaterad brandvägg och virusskydd.

För mer information hänvisas till avsnitten ”Informationskontroll” och ”Regler och begränsningar” i Lisebergs IT-direktiv.

7. Styrning av åtkomst

För att förhindra obehörig användning eller åtkomst av känslig information har Liseberg ett system för behörighetskontroll av åtkomstskyddad information. Syftet är

att kontrollera användningen så att endast de som behöver uppgifterna i sitt arbete får tillgång till åtkomstskyddad information.

Vid tilldelning och kontroll av behörighet skall följande tillämpas:

Standardbehörighet – Denna behörighetsgrad är indelad i olika kategorier på gruppbasis där Lisebergs IT-avdelning styr vilken åtkomst som skall medges en särskild grupp av anställda. Åtkomsträttigheter till informationshanteringssystem skall vara knutna till och definierade av affärsmässig/organisatorisk roll och befattning.

Accessbegäran – För åtkomsträttigheter innefattande standardbehörighet, enligt ovan, e-post samt utökad behörighet skall en skriftlig accessbegäran lämnas till avdelningschef IT. Vidare gäller att:

Användarkoder är personliga och varje användare har ansvar för sin personliga användar-ID och därtill hörande lösenord och för att dessa inte kan missbrukas.

Åtkomsträttigheter ger endast rätt till information som krävs av affärsmässiga skäl, även om det tekniskt sett ger tillgång till ytterligare information.

Som IT-användare på Liseberg har man ett personligt ansvar att informera systemägare vid behov av förändring och borttagning av behörigheter.

8. Säkerhet för e-post

E-postadressen skall alltid vara betecknande, det vill säga mottagaren skall med lätthet kunna identifiera avsändaren.

Användning av e-post får endast ske i enlighet med Lisebergs vid var tid gällande IT-direktiv.

För mer information se avsnitt ”Användning av e-post” i Lisebergs IT-direktiv.

9. Internetaccess

Användning av Internet får endast ske i enlighet med Lisebergs vid var tid gällande IT-direktiv.

För mer information se avsnitt ”Användning av Internet” i Lisebergs IT-direktiv.

10. Skydd av register och handlingar

Liseberg hanterar i sin dagliga verksamhet mängder av register och information lagrad i dessa. Många av dessa register omfattas av lagkrav och/eller affärsmässiga konfidentialitetskrav.

För att skydda dessa register gäller följande:

- En förteckning över vilka register som omfattas av lag- och/eller konfidentialitestkrav skall upprättas och hållas uppdaterad.
- Ansvarig för registret är Lisebergs personuppgiftsombud.
- Ansvarig för att hålla förteckningen aktuell är respektive registeransvarig/systemägare i samråd med Lisebergs personuppgiftsombud.
- Skyddskrav för registret, bland annat hur länge det skall sparas och eventuella krav på hur det skall sparas skall fastställas.

Som exempel kan nämnas att all persondata skall förvaras av personaladministratör i låsbart brandskyddat skåp.

11. Skydd av persondata

Sverige liksom många andra länder har valt att lagstifta i syfte att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter. Lagstiftningen tar bl.a. ställning till när behandling av personuppgifter är tillåten samt vilka krav som ställs på de som behandlar personuppgifter.

För allt arbete inom Liseberg gäller att lokala lagar och förordningar skall efterlevas vilket i detta specifika fall för Sverige bland annat är Personuppgiftslagen (”PuL”).

För mer information hänvisas till Lisebergs IT-direktiv.

12. Säkerhetsåtgärder

För att Liseberg skall kunna upprätthålla funktionaliteten hos IT-systemen även i problemsituationer så krävs rutiner och material för att säkerställa och snabbt kunna återställa och återuppta normala aktiviteter. Nedan angivna rutiner och åtgärder syftar till att säkerställa ett gott skydd mot stöld och händelser som kan förstöra utrustningen.

13. Säkerhetskopior

För att möjliggöra ett snabbt återställande och återupptagande av normalt IT-stöd skall säkerhetskopior tas av nödvändigt material som t.ex. databaser, filsystem, program och mjukvara.

Säkerhetskopiorna skall förvaras på ett sådant sätt och på sådan plats att man i händelse av brand, eller på annat sätt totalförstörda system, har möjlighet att starta om IT-systemen utan att behöva tillgång till den ursprungliga miljön. Rutinerna för omstart skall vara dokumenterade och tillgängliga tillsammans med säkerhetskopior.

14. Regler för lösenordshantering

Lösenordet skall bestå av minst åtta tecken varav minst tre av de fyra teckenalternativen:

- Små bokstäver
- Stora bokstäver
- Siffror
- Specialtecken (t ex: !#=?-+)

Exempel: Maj2016!

Lösenordet gäller i 90 dagar och du får en påminnelse att ändra det 7 dagar innan det går ut.

Du får inte ändra lösenordet till något av de du haft de senaste 24 gångerna.

Lösenordet kan inte bytas igen förrän efter 4 dagar.

15. Loggning av händelser

Intrång i IT-system eller andra avvikelser från IT-säkerhetsdirektivet kan vålla stor skada. Liseberg skall därför aktivt agera för att på ett tidigt stadium upptäcka och skydda sig mot sådana händelser.

Vid besök på Internetsidor går det att utläsa varifrån besöket kommer, vilket medför att det är Liseberg som står som avsändare. Då sådana händelser oftast lämnar spår i olika loggar så skall loggningen i Lisebergs IT-system och nätverk vara organiserad så att händelser av denna karaktär loggas.

Liseberg skall logga såväl information utifrån åtkomst som relaterad till utskrifter och filhantering. Loggad information arkiveras för en period om tre månader.

Det skall dessutom finnas dokumenterade rutiner för protokollförda genomgångar av loggar och uppföljning av eventuella händelser som indikerar intrångsförsök och brott mot detta IT-säkerhetsdirektiv och/eller Lisebergs IT-direktiv.

Avdelningschef IT:

- ansvarar för att loggning sker
- ansvarar för att dokumenterade rutiner för regelbunden genomgång och uppföljning av loggar finns
- är sammankallande till regelbundna genomgångs- och uppföljningsmöten
- ansvarar för att mötena genomförs och protokollförs
- ansvarar för att beslutade uppföljningsåtgärder genomförs
- ansvarar för att personalen kontinuerligt informeras om eventuella förändringar i detta IT-säkerhetsdirektiv eller Lisebergs IT-direktiv.

För mer information se även avsnitt ”Informationskontroll” i Lisebergs IT-direktiv.

16. Utbyte av information och program

Liseberg utbyter regelmässigt konfidentiell och affärskritisk information med andra organisationer och eventuellt personer.

Det är därför av största vikt att denna information hanteras på ett sätt som garanterar en hög stabilitet, en tillräcklig kapacitet och en säkerhetsnivå som gör att Liseberg kan garantera konfidentialitet, kvalitet och tillgänglighet till system och behövliga data för sådana samarbetspartners.

17. Säker avveckling

När fasta eller löstagbara lagringsmedier som innehåller konfidentiell information eller personuppgifter inte längre skall användas för sitt ändamål skall lagringsmedierna förstöras eller raderas på sådant sätt att uppgifterna ej kan återskapas. Utrustning som t.ex. hårddisk på arbetsstationer eller servrar som har varit i internt bruk på Liseberg innehåller alltid konfidentiell data och annan kritisk information (t.ex. lösenord) samt Liseberg-licenserad programvara.

Hårddisken på alla arbetsstationer eller servrar som har varit i internt bruk och som avvecklas eller säljs skall därför rensas med ett kvalificerat diskrensnings-mjukvara, vilket skall hanteras av IT-avdelningen.

IT-avdelningen kan delegera uppgiften till annan kvalificerad personal.

18. Bärbara datorer

Bärbara datorer kräver särskilt höga krav på säkerhet då risken att personuppgifter eller annan för företaget eller individer känslig information kan kommas åt av utomstående.

En bärbar dator är ett begärligt stöldobjekt och skall förvaras ej synligt på arbetsplatsen efter arbetstid. Om datorn tas med från arbetsplatsen så skall den förvaras på säkert sätt.

19. Konsekvenser av brott mot direktiv

Ansvarig chef är ansvarig för att varje misstänkt brott mot detta IT-säkerhetsdirektiv anmäls till avdelningschef IT. Beroende på hur allvarligt brottet är kan följande sanktioner komma ifråga.

- Begränsad tillgång till e-post.
- Begränsad tillgång till Internet, d.v.s. endast till vissa specifika adresser.
- Ingen Internet-tillgång alls.

En överträdelse av allvarlig art kan leda till skadeståndsanspråk och uppsägning, är överträdelsen av mycket allvarlig art kan det leda till avsked, polisanmälan och åtal.