LISEBERG

IT-direktiv för Lisebergs medarbetare

Antaget den 30 juni 2016 av styrelsen för Liseberg

1. Inledning

Detta direktiv beskriver de villkor under vilka medarbetare får ~~ut~~nyttja Lisebergs IT-resurser.

För utförande av arbetsuppgifterna tillhandahåller Liseberg datorer, mjukvaruprogram samt i vissa fall e-post och Internet-uppkoppling. Dessa arbetsredskap är till för att stödja medarbetaren i det dagliga arbetet. All information som finns lagrad tillhör Liseberg.

Liseberg är beroende av sitt goda rykte. Liseberg kan därför inte acceptera att bolagets namn förekommer i några sammanhang som kan skada dess anseende hos allmänhet, kunder eller kollegor.

Medarbetare får endast använda de IT-resurser som tilldelats medarbetaren utifrån vederbörandes roll och arbetsuppgifter. Medarbetaren får inte försöka bereda sig tillgång till andra system eller programvaror än de som medarbetaren fått tillgång till av IT-avdelningen.

Medarbetaren har ett personligt ansvar att informera sig om de regelverk, rutiner och det ansvar som är tillämpliga.~~Medarbetaren får inte ta del av information lagrad på gemensamma datorresurser annat än i den omfattning som krävs för utförande av medarbetarens arbetsuppgifter.~~

Instruktioner och anvisningar från IT-ansvariga skall alltid följas.

2. Hantering av personuppgifter

Liseberg behandlar, i den utsträckning som krävs för att fullgöra Lisebergs skyldigheter som arbetsgivare enligt lag och avtal, sina medarbetares personuppgifter. Denna databehandling begränsar sig till sådana personuppgifter som omfattas av § 10 och 16 i personuppgiftslagen (PuL).

Efter överenskommelse med medarbetaren lagrar bolaget även uppgifter om dennes erfarenhet och kompetens i form av en individuell CV i ett HR-system.

Medarbetaren kan alltid vända sig till Liseberg och begära att ofullständig eller felaktig information om medarbetaren kompletteras eller rättas.

Om medarbetaren avslutar sin anställning på Liseberg kommer Liseberg, på begäran från medarbetaren, tillse att all information rörande denne som Liseberg inte måste spara för att kunna fullgöra dess skyldigheter enligt lag och avtal, raderas.

3. Användning av Internet

Liseberg tillhandahåller en Internettjänst som skall användas i tjänsten eller för sådan kompetens- och kunskapsutveckling som Liseberg stödjer.

Användningen skall stå i överenskommelse med regler, direktiv och interna anvisningar.

Lisebergs Internettjänster får inte användas för:

- uppkoppling och hemtagning av material som kan tillfoga Liseberg skada, negativ publicitet eller ersättningsskyldighet
- ~~uppkoppling till och hemtagning av material som är kränkande eller diskriminerande, det vill säga material som innehåller pornografi, rasism, nazism eller liknande~~
- uppkoppling till och nedladdning av programvaror

Vid besök på Internet går det att utläsa varifrån besöket kommer och därmed är det Liseberg som står som avsändare. Internet-sidor med innehåll som är olagligt eller kan väcka anstöt får aldrig – inte ens utanför arbetstid – besökas eller eftersökas. Liseberg får under inga omständigheter förekomma i några sammanhang som kan skada Lisebergs anseende hos allmänhet, kunder eller kollegor.

Att hämta hem program och annat från Internet kan innebära risker för Liseberg. Detta gäller dels på grund av risken för datavirus, dels på grund av att hämtad programvara kan störa övriga installerade program och förorsaka fel eller allmänt belasta systemet. Därför är all nedladdning av programvara från Internet förbjudet.

Det är inte tillåtet att göra personliga inköp via Internet från Lisebergs datorer. Det är inte heller tillåtet att utföra privata bankärenden eller liknande från Lisebergs datorer. Liseberg skall inte på något vis kunna bli ansvarigt för gjorda inköp eller andra dispositioner och Lisebergs adress får inte användas i sådana sammanhang.

4. Användning av ~~E~~e-post

~~Elektronisk post är ett effektivt sätta att sprida och utbyta information.~~ Liseberg tillhandahåller ett e-postsystem som skall användas för att stödja verksamheten och Lisebergs mål.

Vid regelbunden kommunikation som kräver stora datautrymmen bör ~~koncernens~~Lisebergs ~~intranät~~ verksamhetsportal användas och inte e-postsystemet.

Vid säsongsanställning ingår inte e-postadress, utan sådan beviljas vid behov.

Antaget den 30 juni 2016 av styrelsen för Liseberg

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

Lisebergs ~~E~~e-postsystem får inte användas för:

- personlig vinning
- att få tillgång till programvara eller dylikt som man inte har licens för
- ~~meddelanden med politiskt eller religiöst innehåll eller propaganda i någon form~~
- ~~budskap som är kränkande, diskriminerande eller är olagligt, det vill säga meddelanden som innehåller pornografi, rasism, nazism eller liknande~~
- försändelse av e-post av kedjebrevs karaktär
- ~~onödigt många och stora filer som belastar bandbredd och diskutrymme~~automatisk extern vidarebefordran[2] av Lisebergs e-post
- Hantering av information som är klassad i nivå 2[3] avseende konfidentialitet (sekretess) och riktighet utan vederhäftiga kryptografiska funktioner i e-posten[4].
- att medverka till ”spamming”, d.v.s. spridande av irrelevant information över stora grupper på nätet

Den som använder sig av e-post skall:

- skicka meddelanden under eget namn
- endast läsa meddelanden som är adresserade till sig själv eller på tydligt uppdrag av någon
- inte ändra i meddelanden som vidarebefordras utan att markera ändringarna
- kontrollera sin e-post minst en gång per dag, varje helgfri måndag till fredag. Medarbetare som inte ger fullmakt till någon annan att ha tillgång till den egna e-posten är själv ansvarig att kontrollera e-posten även vid frånvaro såsom semester, barnledighet, sjukskrivning etc.
- I sin e-post skilja ut och utan dröjsmål hantera allmänna handlingar[1] enligt gällande regelverk såsom informationsklassificering, registrering/diarieföring, arkivering etc
- Säkerställa att det finns gallringsbeslut innan någon allmän handling eller uppgift förstörs eller raderas
- löpande tillse att oönskad e-post raderas ur systemet

5. Lösenord

Det är medarbetarnas skyldighet att känna till och följa den vid var tid gällande rutinen för hantering av lösenord. Liseberg äger rätt till samtliga lösenord som används i datasystemet.

Liseberg har genom IT-support tillgång till all information som finns lagrad på datorernas hårddisk och bolagets servrar. Användande av lösenord innebär således inte att det skapas något privat utrymme i datorn.

6. Informationskontroll

Datorer och servrar ägs av Liseberg. Nedladdning och lagring av material på dessa i annat än obetydlig omfattning får endast ske avseende sådant material som har samband med arbetet.

Liseberg skall ha tillgång till all information inom systemen vilket innebär att ingen information får blockeras för åtkomst, exempelvis genom kryptering.

Liseberg har rättslig skyldighet att utöva kontroll över sina IT-system, till exempel för att tillse att Liseberg följer de bestämmelser som anges i personuppgiftslagen, lagen om ansvar för elektroniska anslagstavlor eller att tillse att Liseberg inte bryter mot upphovsrättslagen. Liseberg kan också kontrollera sina IT-system, inklusive e-post skickat till och från Lisebergs system, för att upptäcka och motverka virus och intrångsförsök eller, för att utreda misstanke om brott eller illojalt beteende.

All användning av Internet och datorn registreras därför i logg. Loggningen används endast i syften beskrivna i detta IT-direktiv.

Vad gäller loggning avseende Internet, filöverföring och e-post omfattar loggen följande uppgifter.
Internet: Användare, adress (URL) på besökt webbplats, tidpunkt för besök och IP-nummer.
Filöverföring: Avsändare och användare, mottagare, storlek och namn på fil samt tidpunkt.
E-post: Avsändare, mottagare, ärende rad, storlek på meddelandet, namn på eventuella bifogade filer och tidpunkt.

Vad gäller loggning avseende datoranvändning, omfattar loggningen inlogg och åtkomster till system, filer och utskrifter m.m.

Loggarna bevaras under tre månader och vid utredning, så länge utredningen pågår.

Liseberg utför slumpvisa stickprovskontroller och övervakar dagligen datanätet i syfte att tillse att detta direktiv följs, för att uppfylla sina rättsliga skyldigheter och för att upprätthålla god IT-säkerhet. IT-avdelningen håller veckovisa IT-säkerhetsmöten, där loggar, systemstatus, nyttjande samt virus- och övriga angreppsförsök följs upp. Avdelningschef IT rapporterar avvikelser till funktionschef HR eller VD.

En enskild person kan komma att kontrolleras efter beslut av VD eller funktionschef HR. En sådan kontroll kan inledas vid misstanke om brott mot detta direktiv, till exempel om loggen indikerar onormalt hög icke-arbetsrelaterad surfning eller surfning på otillåtna webbplatser, eller om det föreligger allvarlig misstanke om illojalt eller brottslig beteende. Vid allvarlig misstanke om illojalt eller brottsligt beteende eller allvarlig misstanke om brott mot detta direktivs punkt 3 och 4 kan även e-post och filer av privat natur komma att granskas, vilket annars undviks i möjligaste mån.

Det är förbjudet att:

- försöka tränga igenom interna eller externa säkerhetsspärrar
- låta annan anställd, anhörig eller bekant låna lösenord och användarnamn
- låta anhörig eller bekant låna Lisebergs datorer
- koppla in extern IT-utrustning i Lisebergs nät
- kopiera eller arkivera material från Lisebergs IT-system, exempelvis kundregister eller uppgifter om Lisebergs besökare

7. Regler och begränsningar

Det är förbjudet att installera programvara utan att IT-avdelningen är underrättad och har givit sitt godkännande. Alla IT relaterade inköp skall också godkännas av avdelningschef IT.

Medarbetarna inom Liseberg äger ingen rätt att installera om eller förändra installerade program.

Det är inte tillåtet att ladda ner dokument eller filer som tillhör Liseberg på privata lagringsmedia och ta med detta material till annan dator utanför Liseberg.

Hjälpmedel och verktyg tillhandahållna av Liseberg är Lisebergs egendom.

Privat användning av Lisebergs IT-system får endast ske i mycket begränsad omfattning och får inte påverka ordinarie arbetsuppgifter eller inverka menligt i form av kostnader, lagringsutrymme, prestanda etc

För att minska miljöpåverkan skall Lisebergs medarbetare:

- stänga av kontorsdatorn och bildskärmen när man lämnar arbetsplatsen för dagen.
- hantera utskrifter varsamt

Lisebergs IT-resurser får inte användas för ändamål som kan uppfattas som oetiskt eller stötande t.ex. hantering av information och material som är pornografiskt,

Antaget den 30 juni 2016 av styrelsen för Liseberg

diskriminerande eller har anknytning till kriminell verksamhet. Undantag från detta kan göras i de fall sådan information/material behövs för tjänstebruk, vilket skriftligen ska godkännas av VD.

8. Åtgärder vid brott mot detta direktiv

Ansvarig chef är ansvarig för att varje misstänkt brott mot detta direktiv 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.

.

NOTER

1. Innehållet avgör alltid om en handling är allmän eller inte. Om e-postmeddelandet berör Lisebergs verksamhet blir meddelandet allmän handling direkt när det är inkommet. Den information om meddelanden som finns i loggar/förteckningar utgör alltid allmän handling. Den e-post som utväxlas internt inom en verksamhet mellan medarbetare såsom utkast, koncept eller annat internt arbetsmaterial är normalt inte allmän handling
2. Med extern vidarebefordran menas att e-post som ska hanteras i Lisebergs e-postsystem istället med automatik skickas vidare och hanteras i ett e-poststssystem som finns utanför Lisebergs nät och utanför Lisebergs kontroll. Exempel på sådana e-postsystem är Hotmail och Gmail
3. Exempel på information i nivå 2 är känsliga personuppgifter enlig PuL eller sekretessbelagd information. För mer information hänvisas till respektive systems systemsäkerhetsplan samt Lisebergs IT-avdelning.
4. De kryptografiska funktionerna bör ligga i nivå med nationellt godkända kryptografiska funktioner. Kontakta Lisebergs IT-avdelning för stöd och mer information.

Antaget den 30 juni 2016 av styrelsen för Liseberg

Liseberg