IT-DIREKTIV FÖR LISEBERGS MEDARBETARE

Antagen den XX juni 2022 av styrelsen för Liseberg

1. Inledning

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

För utförande av arbetsuppgifter tillhandahåller Liseberg IT-resurser såsom; datorer, telefoner, mjukvaruprogram, e-post och Internet-uppkoppling. Dessa arbetsredskap är till för att stödja medarbetaren i det dagliga arbetet. All information som finns lagrad på Lisebergs datorer och servrar 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. Privat användning får endast ske i mycket begränsad omfattning och får inte påverka ordinarie arbetsuppgifter eller inverka menligt på Lisebergs IT-resurser i form av kostnader, lagringsutrymme, prestanda etcetera.

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.

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 personuppgiftbehandling hänvisas till Dataskyddsförordningen (EU) 2016/679, även kallad GDP), till Artikel 6, skäl 40 – 50, *Laglig behandling av personuppgifter*.

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

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 Internetaccess 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 Internetaccess får inte användas för:

- uppkoppling och hemtagning av material som kan tillfoga Liseberg skada, negativ publicitet eller ersättningsskyldighet

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. Nedladdning av program till Lisebergs IT-utrustning skall i första hand göras från programbibliotek anvisade av Lisebergs IT-avdelning. Därför är all nedladdning av programvara från Internet förbjudet.

4. Användning av e-post

Liseberg tillhandahåller ett e-postsystem som skall användas för att stödja verksamheten och Lisebergs mål. Känsliga personuppgifter [1] ska alltid skickas med

[1] Känsliga personuppgifter är: Ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska personuppgifter, biometriska personuppgifter (GPS), personuppgifter om hälsa, sexuell läggning eller sexuella vanor.

kryptering, tänk också på att inte spara känsliga personuppgifter i din Outlook längre än vad specifikt ärende kräver, se mer i dokumenthanteringsplanen.

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

Lisebergs e-postsystem får inte användas för:

- personlig vinning
- att få tillgång till programvara eller dylikt som man inte har licens för
- försändelse av e-post av kedjebrevskaraktär
- 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 enligt gällande regelverk såsom informationsklassificering, registrering/diarieföring, arkivering etc

---

[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-postssystem 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 (se punkt 5) enlig dataskyddsförordningen 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.

Antagen den XX juni 2022 av styrelsen för Liseberg

- Säkerställa att det finns gallringsbeslut innan någon allmän handling eller uppgift förstörs eller raderas
- Löpande tillse att oönskad e-post raderas ur systemet i enlighet med dokumenthanteringsplanen.
- Löpande tillse att radera personuppgifter i din e-post som inte längre fyller något syfte.

5. Lösenord

Det är medarbetarnas skyldighet att känna till och följa den vid var tid gällande rutinen för hantering av lösenord samt skydda de lösenord, pinkoder etcetera som erhållits för åtkomst. Medarbetaren skall konstruera lösenord så att de inte lätt går att pröva sig fram till eller gissa samt omedelbart byta lösenordet om det kan misstänkas att någon annan känner till det. Lösenord är personliga och får ej delas med andra. Liseberg äger rätt till samtliga lösenord som används i datasystemet.

6. Informationskontroll

IT-utrustning 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 annan kryptering än den som Lisebergs IT-avdelning aktiverat.

Liseberg har rättslig skyldighet att utöva kontroll över sina IT-system, till exempel för att tillse att Liseberg följer de bestämmelser som anges i dataskyddsförordningen, 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 IT-utrustning registreras därför i logg. Loggningen används endast i syften som är beskrivna i detta IT-direktiv.

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 regelbundet IT-säkerhetsmöten, där loggar, systemstatus, nyttjande samt virus- och övriga angreppsförsök följs upp. Avdelningschef IT rapporterar avvikelser till funktionschef People & Culture eller VD.

Antagen den XX juni 2022 av styrelsen för Liseberg

Liseberg

En enskild person kan komma att kontrolleras efter beslut av VD eller funktionschef People & Culture. 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

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 IT-utrustning
- koppla in extern IT-utrustning i Lisebergs nät
- kopiera eller arkivera material från Lisebergs IT-system, exempelvis kundregister eller uppgifter om Lisebergs besökare
- kopiera copyrightförsedd information utan godkännande eller använda den på ett sådant sätt att en annan organisation otillåtet kan nyttja Lisebergs information eller programkod

7. Regler och begränsningar

Införande av nya system och programvaror (även molntjänster) skall alltid ske i samråd med, och godkännas av Lisebergs IT-avdelning. Alla IT-relaterade inköp skall godkännas av IT-chef.

Medarbetaren ansvarar själv för att datorapplikationer och mobilappar för personligt bruk inte utgör en säkerhetsrisk för Lisebergs IT-miljö. Nedladdning skall i första hand ske från de applikationsportaler som tillhandahålls av Lisebergs IT-avdelning.

Medarbetaren skall informera ansvarig vid behov av förändring och borttag av behörigheter.

Hjälpmedel och verktyg tillhandahållna av Liseberg är Lisebergs egendom.

Medarbetaren skall till IT-avdelningen direkt rapportera störningar eller avvikelser i säkerheten eller om man fått meddelande till exempelvis epost eller sms som strider mot lagar och förordningar

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

Antagen den XX juni 2022 av styrelsen för Liseberg

Liseberg

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, 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.

Informationsspridning med hjälp av IT (såsom epost, webbsidor, bloggar etcetera) som inte ingår i ordinarie arbetsuppgifter från Liseberg ska inte formuleras så att de som läser får uppfattningen att informationsspridningen sker på uppdrag av Liseberg.
Medarbetaren ska förhindra att obehöriga kan använda IT-resurser och information samt hantera anförtrodd IT-utrustning på ett sådant sätt att stöld och obehörig åtkomst förhindras.

IT-utrustning skall alltid hanteras varsamt och under transport skyddas med väska eller skal.

För att minska miljöpåverkan skall Lisebergs medarbetare:

- försätta dator/skärm i viloläge när man lämnar arbetsplatsen för dagen.
- begränsa antalet utskrifter i möjligaste mån

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 i fråga.

- 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.

Antagen den XX juni 2022 av styrelsen för Liseberg