Lyyti Informationssäkerhet

Att upprätthålla en hög nivå av informationssäkerhet är vår högsta prioritet. När du anförtror din eventdata till Lyyti kan du vara säker på att den är trygg. Vi är till 100 % engagerade i att upprätthålla strikta säkerhetsstandarder genom flera skyddslager.

Med Lyyti har du alla verktyg som behövs för att hantera din deltagardata på ett säkert sätt.

Lyytis informationssäkerhetssystem (ISMS) har utformats i enlighet med ISO/IEC 27001-standarder och omfattar ett brett spektrum av säkerhetsåtgärder. Dessa åtgärder inkluderar kontroller, policys, riktlinjer, planer och procedurer, alla utformade för att skydda varje aspekt av vår verksamhet.

- Lyyti behandlar endast data inom EU:s gränser, i enlighet med GDPR (2016/679).
- Alla Lyytis lokaler är anpassade och utrustade för att uppfylla mycket strikta säkerhetsbestämmelser.
- Lyytis system övervakas dygnet runt av vårt driftsteam, varje dag året runt. Detta för att snabbt kunna identifiera och åtgärda potentiella sårbarheter.
- Alla våra underleverantörer är noggrant utvalda för att kunna matcha våra höga säkerhetsstandarder. Varje underleverantör granskas årligen för att säkerställa efterlevnad. Du hittar alla våra underleverantörer här.
- Lyytis säkerhetskopieringssystem täcker fyra olika operativa nivåer som är geografiskt åtskilda, för att öka säkerheten.
- Vårt säkerhetsprogram för all personal kräver att alla anställda genomgår årlig utbildning i datasäkerhet och dataskydd, vilket säkerställer att vårt team är väl insatt i att upprätthålla de högsta standarderna för informationssäkerhet.

Lyytis säkerhetsprogram

Företagssäkerhet omfattar alla aspekter av företagets verksamhet. Vårt säkerhetsprogram hjälper oss att skydda Lyytis kärnvärden, inklusive människor, data, rykte, egendom, tillgångar och miljön. En av säkerhetsprogramets främsta uppgifter är att stärka företagets konkurrenskraft genom att säkerställa konfidentialitet, integritet och tillgänglighet för all behandlad information. Våra anställda genomgår därför årligen utbildningar inom datasäkerhet och dataskydd.

Fysisk säkerhet

Lyytis kontor är utrustade med elektroniska lås, kameraövervakning och moderna inbrottslarmssystem samt övervakas dygnet runt av ett externt säkerhetsföretag. Varje anställd måste använda en personlig elektronisk nyckel för att få tillträde till kontoret. Alla åtkomsthändelser loggas, övervakas och kan granskas vid behov.

Driftleverantören för Lyytis produkter följer flera branschkända säkerhetsstandarder, såsom ISO 9001, SOC 1 Typ II, SOC 2 Typ II, ISO 27001, ISO 22301 och PCI-DSS. En omfattande lista över värdleverantörens certifieringar hittar du här.

Dataklassificering

Lyyti använder en dataklassificeringsmodell med tre nivåer. Kriterierna för att klassificera data till dessa nivåer, tillsammans med riktlinjer för hantering av varje klassificeringsnivå, beskrivs i vår policydokumentation. Anställda får regelbunden utbildning i dessa rutiner för att säkerställa korrekt datahantering.

Ändpunktssäkerhet

Alla enheter som får åtkomst till företagets data har genomgåtts av företaget och har säkrats på ett dokumenterat sätt. Dessa enheter skyddas mot olika typer av attacker med en XDR-lösning som övervakas dygnet runt. Lyyti använder en MDM-lösning för att kontrollera och uppdatera vår ändpunktspolicy, vilket säkerställer att alla enheter hanteras och krypteras. Användare är skyldiga att rapportera eventuella avvikelser som uppstår vid användning av företagets enheter.

"Lyyti Acceptable Use Policy" beskriver godtagbar användning av företagets IT-resurser och företagsutgivna tillgångar och inkluderar processen för policyöverträdelser.

Säkerhetsutbildning

Alla nya medarbetare måste genomgå säkerhets- och sekretessutbildning samt klara ett slutprov sin första arbetsdag. Utbildningsinnehållet uppdateras regelbundet och all personal är skyldig att vara uppdaterade på det senaste och klara motsvarande prov inom angivna tidsramar, normalt minst en gång per år. Resultaten av dessa prov övervakas och registreras noggrant för ansvarighetsändamål.

Utvecklare utbildas årligen i praxis för säker programvaruutveckling.

Datakryptering

Alla företagsutgivna enheter är krypterade. Kunddata behandlas alltid i krypterad form, både när den lagras och under överföring.

Företagets säkerhetsroller

Alla säkerhetsrelaterade roller och tillfälliga ersättare finns angivna på Lyytis interna företagssidor. Företagets säkra kommunikationskanaler inkluderar kontaktuppgifter till innehavarna av säkerhetsroller.

Policybeskrivning

Företagets säkerhetsdokumentation består av flera kontrollerade policydokument och riktlinjer, som alla tilldelats en utsedd ägare med huvudansvar för granskningsprocessen. Dessa dokument genomgår en årlig granskning, eller vid någon betydande ändring av innehållet. Detta system säkerställer att policys och riktlinjer förblir aktuella och går i linje med organisationens mål, syften och lagkrav.

Säkerhetsincidenter och hantering

Lyyti upprätthåller dokumenterade processer och omfattande planer för incidenthantering, vilket säkerställer kontinuerlig övervakning av säkerhetsincidenter och lösningar. Alla anställda är skyldiga att omedelbart rapportera eventuella upptäckta eller misstänkta överträdelser av vår informationssäkerhetspolicy, intrångsförsök, dataintrång, stöld eller förlust av hårdvara samt andra säkerhetsrelaterade händelser och incidenter.

Vi granskar regelbundet vår dokumentation för incidenthantering och gör den tillgänglig för alla användare. Dokumentationen beskriver kommunikationsprotokoll som ska följas under incidenter och betonar vikten av snabba åtgärder för att skydda Lyytis tjänster och data.

Riskhantering

Riskhantering är en integrerad del av Lyytis strategiska process. Det hjälper oss att uppnå våra mål genom att säkerställa att riskerna är proportionerliga till riskkapaciteten.

Vi har identifierat och dokumenterat olika risker i ett register. Riskerna har klassificerats och analyserats, och åtgärdsplaner upprättas årligen för att minska riskerna. Vår CTO tillsammans med VD och Compliance-teamet, är ansvariga för att formulera riskhanteringspolicyn och riskbedömningen. Ledningsgruppen godkänner riskhanteringspolicyn och granskar processen årligen.

Business Continuity Plan (BCP) och Disaster Recovery Plan (DRP)

Lyyti har en Business Continuity Plan som stöds av en omfattande Disaster Recovery Plan. Detta säkerställer att alla kritiska affärsfunktioner kan fortsätta både under och efter en katastrof. Huvudmålet med Disaster Recovery Plan är att minimera systemavbrott och dataförluster. Dessa dokument granskas regelbundet för att säkerställa deras effektivitet.

Sårbarhetsskanningar och övervakning

Hela Lyytis infrastruktur genomgår operativ övervakning dygnet runt, inklusive molninfrastruktur, nätverk, slutpunkter och kontorsfastigheter. Eventuella avvikelser som upptäcks klassificeras, dokumenteras och hanteras enligt policyer och riktlinjer. Alla miljöer skannas även efter sårbarheter: online, dagligen eller veckovis, beroende på systemet.

Penetrationstestning

Ett oberoende externt företag genomför penetrationstestning minst en gång per år. Alla möjliga upptäckter dokumenteras i de elektroniska systemen och hanteras på ett lämpligt sätt.

En sammanfattning från det senaste penetrationstestet, utfört av Fraktal Oy i mars 2024, hittar du här.

Patchhantering

Lyytis drifthårdvara och programvara övervakas kontinuerligt för potentiella sårbarheter. Sårbarheter som klassificeras som "Kritiska" eller "Höga" enligt CVSS v3.0 Severity Rating system patchas omedelbart, medan de som klassificeras som "Medelhöga" eller lägre patchas inom en månad efter att patchen släppts.

Säkerhetsrutiner för anställda och leverantörer

Lyyti är dedikerade till att upprätthålla de högsta säkerhetsnivåerna, med start i anställnings- och introduktionsprocesserna för både anställda och leverantörer. Företaget anställer endast individer som är pålitliga och varje anställningsavtal innehåller dessutom en sekretessklausul för att skydda känslig information.

För att säkerställa hög säkerhet genomgår personal och leverantörer utbildning och måste klara slutprov innan de får tillgång till systemen. Åtkomst är strikt reglerad baserat på arbetsroller, vilket endast tillåter nödvändig åtkomst till känslig data.

Dessutom är alla medarbetare, som en del av deras anställnings- eller kontraktsavtal, skyldiga att följa företagets säkerhetspolicyer. Denna strikta dedikation till säkerhetsrutiner och policyer hjälper Lyyti att skydda sina tillgångar, data och kundernas integritet.

Offboarding för anställda

När en anställd lämnar företaget har vi en detaljerad steg-för-steg-process för offboarding. Detta inkluderar bland annat att användarkontot till alla system som används omedelbart inaktiveras eller raderas samt att de använda enheterna rensas. Alla enheter som företaget lämnat ut är listade i tillgångsregistren och samlas in samt hanteras enligt dokumenterade rutiner.

Plats för datalagring eller underleverantörer

All data som behandlas av Lyyti, inklusive underleverantörers data, hanteras inom EU-regionen. En lista över underleverantörer som används av Lyyti finns tillgänglig här. Alla underleverantörer granskas årligen.