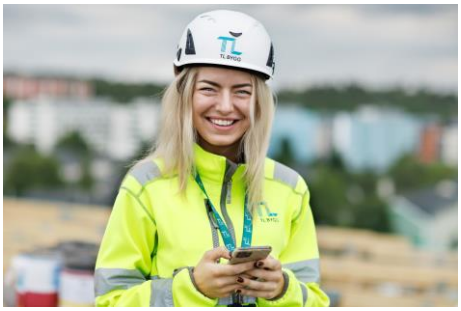
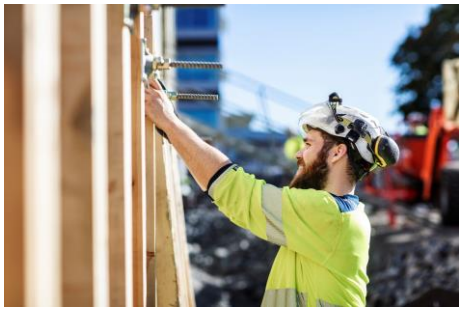




IT- och Cybersäkerhetspolicy

TL Bygg delar IT-avdelning med moderbolaget och speglar deras IT- och Cybersäkerhetspolicy.

Koncernens IT-verksamhet ska bedrivas affärsmässigt, etiskt och säkert med väl etablerade system och modeller som stödjer Koncernens mål och intentioner. IT-baserade verktyg och system är en viktig del i Koncernens kärnverksamhet.

Policyns syfte är att:

- Ha en väl fungerande IT-miljö med hög tillgänglighet som stödjer Koncernens verksamhet
- Fastställa krav för hantering och administration av IT-resurser (molntjänster, system, lösningar, hårdvara, information/data och IT-konsulter) inom Koncernen
- Säkerställa en hög nivå i Koncernens Cybersäkerhet (IT- och Informationssäkerhet)

Inköp

Inköp av nya IT-resurser (molntjänster, system, lösningar, hårdvara och IT-konsulter) ska ske centralt av IT. Förslag på inköp meddelas IT som bereder och godkänner.
IT tillhandahåller en standardarbetsplats, extra utrustning kräver godkännande av närmaste chef och bekostas av beställaren.

Metod för projekt/inköp/systemutveckling

Valda projekthanterings-, inköpshanterings- och systemutvecklingsmetoder måste inkludera följande moment:

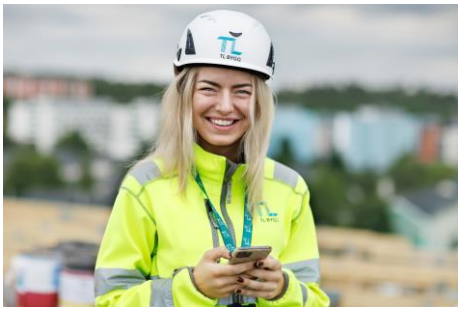
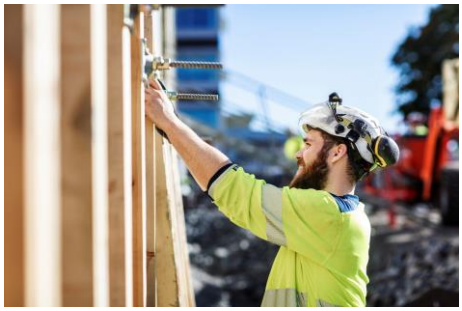
- Säkerhetskrav (inklusive sekretess, integriteten och tillgänglighet)
- Konsekvensanalys med avseende på skydd av den personliga integriteten
- Typ av personuppgifter och behandling
- Design, testning och implementering

Dokumentation skall leva upp till och följa den valda systemförvaltningsmodellens krav.

En systemförvaltningsmodell skall finnas dokumenterad för utveckling och förvaltning av IT-system. IT-funktionen ansvarar för att denna hålls uppdaterad. En objektägare samt en objektägare IT utsedda av ledningsgruppen skall finnas till alla system. Objektägaren skall utse en förvaltningsledare. Objektägare IT skall utse förvaltningsledare IT.

Acceptabelt användande av bolagets it-resurser

Bolagets IT-resurser (molntjänster, system, lösningar, hårdvara och IT-konsulter) ska användas med syfte som gagnar bolaget. Koncernens IT-resurser får inte användas för att på otillbörligt sätt sprida, förvara, förmedla eller titta på information/material som är oetiskt, olagligt eller oförenligt med företagets värdegrund eller policys. Avyttring av IT-resurser som innehåller eller misstänks innehålla känslig information skall ske på ett säkert sätt.

Bolagets IT-resurser får användas för ringa privat bruk om det inte inkräktar på arbetet, äventyrar säkerheten eller medför kostnader för Koncernen. Endast program och filer som är bolagsrelaterade får laddas ner och/eller sparas på Koncernens IT-resurser.

Alla aktiviteter som görs av användare kan komma att loggas, sparas och följas upp. Onormalt nyttjande av IT-resurser kan komma att följas upp och berörda informeras.

Tillgänglighet

Ansvarig för IT-resurser (molntjänster, system, lösningar, hårdvara och IT-konsulter) skall ha som målsättning att de är tillgängliga dygnet runt.

Bolaget har ingen acceptans för:

- Undermålig service/leverans eller att affärskritiska system drabbas av avbrott så att verksamheten inte kan serva sina kunder.
- Systemfel som beror på tekniska eller funktionella felaktigheter i vald plattform / applikation

Planerade driftstopp kan förekomma och skall meddelas till berörd verksamhet i god tid.

IT SÄKERHET

Tekniskt skydd

IT-funktionen är huvudansvarig för det tekniska skyddet av IT-resurser i koncernen. Tekniskt skydd mot IT-attacker skall finnas på alla nätverk och all tillämplig IT-utrustning. Det tekniska skyddet skall hållas kontinuerligt uppdaterat för nya säkerhetshot. Särskild vikt skall läggas vid skydd av användarnas digitala identiteter och autentiseringsfunktioner.

Minst vartannat år skall extern granskning, utvärdering eller test av det tekniska skyddet genomföras.

Övervakning

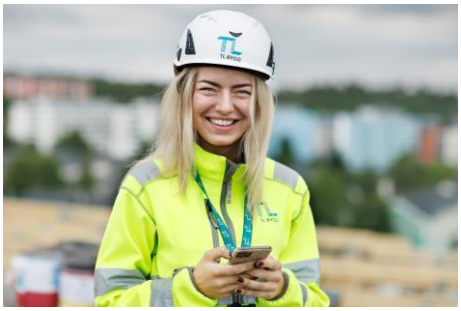
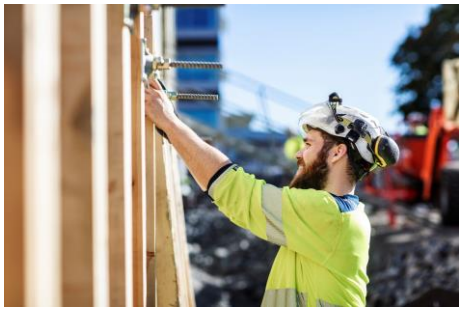
IT-funktionen skall säkerställa att IT miljön och det tekniska skyddet kontinuerligt övervakas för att upptäcka sårbarheter, intrångsförsök, onormala beteenden och skadlig kod.

Incidenthantering

En process för rapportering och hantering av incidenter skall finnas dokumenterad och hållas uppdaterad av IT-funktionen

Kontinuitetsplanering

IT-funktionen skall ha en dokumenterad och testad kontinuitetsplan som säkerställer att affärskritiskt IT återställs inom 48 timmar vid oplanerade störningar och avbrott som inte kunnat förutses (katastrof).

Alla IT tjänster och information som krävs för Koncernens affärsprocesser skall omfattas av kontinuerlig säkerhetskopiering eller motsvarande rutiner för att undvika förlust av data. Maximalt tillåten dataförlust vid återställning från backup vid exempelvis ett allvarligt ransomware scenario är:

- 30 minuters transaktioner/arbete i systemet för affärskritiska system
- 24 timmars transaktioner/arbete i systemet för övriga system

I normalscenario (normal driftstörning eller misslyckad produktionssättning kan förlust av data undvikas helt eller begränsas till de senaste minuternas transaktioner.

INFORMATIONSSÄKERHET

Definition

Informationssäkerhet berör all information och all utrustning för informationshantering som hanteras i Koncernen, exempelvis nedan (men inte begränsad till):

- Lagrad i databas
- Lagrad i en dator och skickad/sänd över ett internt eller publikt nätverk
- Lagrad på ett flyttbart media, som exempelvis USB, SD kort, mm
- Lagrad på ett fast media, som exempelvis hårddisk
- I skrift, som exempelvis handskrivna papper, utskrifter, White boards, mm
- Presentationer, via exempelvis Audio-Visuell media.
- Telefonsamtal, möten eller konversationer
- eller annan kommunikationsmetod

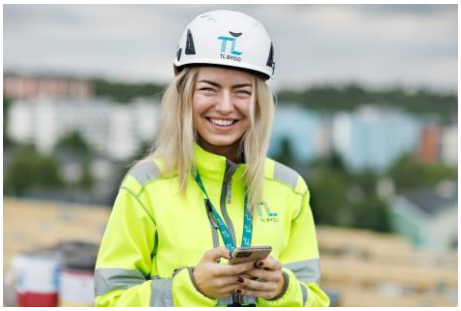
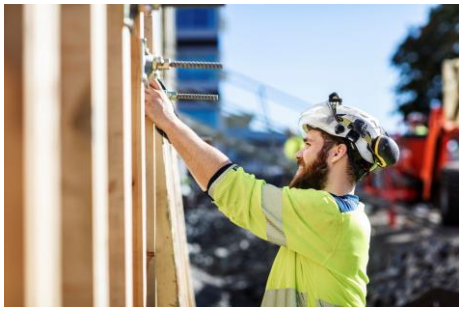
Åtkomst och behörigheter

Behörigheter skall tilldelas behovsbaserat. Personalansvarig chef ansvarar för att medarbetare, inhyrd personal eller konsult erhåller korrekt behörighet och behörighetsnivå till Koncernens IT-resurser (molntjänster, system, lösningar, etc). Personalansvarig chef ansvarar även för att behörighet och behörighetsnivåer tas bort när behovet upphör.

För system-/IT-konsulter ansvarar förvaltningsledare och förvaltningsledare IT för att konsulter inte har mer systembehörighet än vad deras uppdrag kräver. Test och produktionsmiljöer skall vara logiskt separerade.

Hantering av information

All behandling (samla in, sprida, förvara, förmedla, etc) av information skall ske i enlighet med gällande lagstiftning och antagna policy och riktlinjer.

Riskanalys

Objektägare och Objektägare IT skall säkerställa att en riskanalys genomförs:

- Minst en gång per år innefattande systemstöden i respektive Förvaltningsobjekt.
- Innan beslut tas om inköp av applikation/system eller större förändringar av infrastruktur eller applikation/system genomförs

Sekretess

Bolaget har ingen acceptans för säkerhetsöverträdelser eller läckage av information utanför företagets domäner. Information skall skyddas mot obehörig åtkomst och endast vara tillgänglig för behöriga personer samt vara riktig, komplett och aktuell. Koncernens utrustning som innehåller företagsinformation måste skyddas från alla typer av säkerhetsrisker som kan ge obehöriga tillgång till koncernens information, medföra störningar i eller äventyra affärsprocesserna. Egen utrustning får aldrig innehålla eller lagra några informationsmängder som tillhör Koncernen.

Omfattning och efterlevnadsansvar

Personalansvarig chef ansvarar för att informera varje anställd/inhyrd. Koncernen förbehåller sig rätten att kontrollera enskild anställds hantering av IT-resurser (molntjänster, system, lösningar, hårdvara och IT-konsulter) och information om misstankar finns att denna policy inte efterlevs.

Beslut om detta skall informeras VD, HR-chef och moderbolagets CIO.

Om det av kontrollerna framkommer att policyn inte efterlevs kan ärendet komma att utredas. Koncernen kommer i första hand försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden. Vid allvarligare överträdelser kan disciplinära åtgärder komma att vidtas.

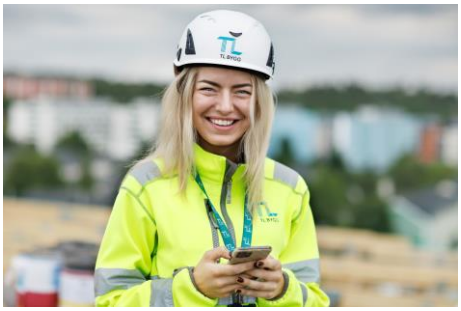
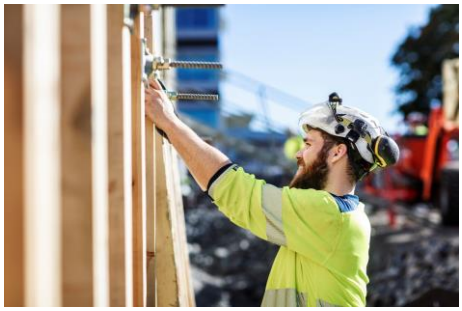
Uppföljning och rapportering (Periodiska kontroller)

Rapportering och uppföljning av efterlevnaden och bevis för att IT policyn med där tillhörande riktlinjers alla punkter är uppfyllda skall genomföras minst årligen av IT-funktionen

Regelbunden kontroll, dokumentation och rapportering av uppfyllnadsgrad inom hela Koncernen skall ske som en integrerad del i det dagliga arbetet inom IT verksamheten.

Rapporteringen sker på uppmaning av företagsledning eller styrelsen och skall som ett minimum innehålla:

- Uppföljningar av kontrollernas effektivitet med underlag för bedömningen.
- Rapportering av incidenter/avvikelser från policyn med beskrivning.
- Åtgärd/er med beskrivning, åtgärdsnytta samt när incident/avvikelse skall vara åtgärdad.
- Uppföljning av utestående åtgärder samt klarrapportering.

Ansvar och styrning

Koncernens IT- och Cybersäkerhetspolicy ska revideras regelbundet och minst en gång per år fastställas av styrelsen. Moderbolagets CIO/IT-chef är dokumentägare och ansvarar för policyn.

Uppdatering

Policyn uppdateras årligen eller vid behov och fastställs av styrelsen och VD.
Senast fastställd / reviderad 2022-12-08.