Informationssäkerhetsspolicy

1 Syfte 2
2 Omfattning 2
3 Policyns innehåll 2
3.1 Informationssäkerhet 2
3.2 IT-säkerhet 3
3.3 Integritet och hantering av persondata . **Error! Bookmark not defined.**
4 Roller och ansvar 4
5 Kriterier för efterlevnad 4
6 Övriga dokument 4

1 Syfte

Syftet med denna policy är att Informationssäkerheten i Balco Group AB med dotterbolag (hädanefter Balco) skyddar alla informationstillgångar inom bolaget och att affärsmålen uppnås.

Informationssäkerhetspolicyn ska säkerställa att:

- Balco hanterar på ett enhetligt sätt
  - informationssäkerhet
  - IT-säkerhet
- Integritetsfrågor och hantering av persondata.
- Vi följer gällande lagar och förordningar.
- Vi har en Informations- och IT-säkerhet som lever upp till de krav som ställs från myndigheter, beställare, anställda samt kunder.

2 Omfattning

Denna policy gäller för samtliga verksamheter (affärsområden, stödjande enheter , staber) och anställda eller inhyrd personal inom Balco Group AB (nedan kallat Balco).

I delägda verksamheter ska representanter för Balco verka för efterlevnad av denna policy.

Undantag eller dispenser från denna policy måste vara klart definierade och dokumenteras. Alla ansökningar om undantag ska lämnas skriftligt till informationssäkerhetsansvarig, som i samråd med koncernens VD är ansvarig för godkännande. Undantag eller begäran om dispens skall åtföljas av en plan för när efterlevnad återigen har uppnåtts.

3 Policyns Innehåll

Informationssäkerhetspolicyn i Balco skall bidra till att verksamhetens mål kan nås och att koncernen är i linje med gällande regelverk och lagstiftning inom området genom att hantera information och integritetsrelaterade risker på ett tillfredställande sätt. Informationssäkerhets-policyn omfattar all information som lagras eller behandlas inom Balco eller i förekommande fall av dess underleverantörer, oavsett media.

3.1 Informationssäkerhet

Informationssäkerheten skall skydda Balcos verksamhet, anställda, kunder och andra intressenter och genom att definiera lämpliga informationssäkerhetskrav baserat på gällande lag-stiftning, förväntningarna från ovan nämnda grupper, god praxis och regelbundna riskbedömningar. Kraven skall säkerställa att korrekt information är tillgänglig, när den behövs, men endast för den avsedda publiken.

- För att skydda sekretess, integritet och tillgång till information ska god praxis tillämpas.
- Strategiska beslut om informationssäkerhet ska fattas av ledningsgruppen för att säkerställa att informationssäkerhetsstyrningen stöder affärsbehoven.
- Balco skall regelbundet utföra riskanalyser och planera lämpliga motåtgärder för att säkerställa en god informationssäkerhet.
- Lokaler och tekniska anläggningar ska skyddas med lämpliga fysiska säkerhetsåtgärder.
- Samtlig personal som berörs av policyn skall regelbundet informeras om riskerna med brister i informationssäkerheten och deras ansvar.
- Vid inköp av IT-tjänster eller resurser skall informationssäkerhetsaspekterna beaktas i kravställningen.

3.2 IT-säkerhet

IT-säkerhet är en väsentlig del av informationssäkerheten och skall säkerställa lämpligt skyddsnivå för de IT-tjänster, IT-system och IT-infrastruktur där information behandlas eller lagras.

- En systemlista skall upprättas för verksamhetskritiska system där systemägare, informationsinnehåll och annan information som behövs för att möjliggöra effektiv IT-säkerhetsstyrning dokumenteras.
- Åtkomstkontroll skall användas för att säkerställa att endast avsedda användare har tillgång till systemen och att tillgången är relevant för deras roll.
- Balco skall regelbundet utföra behörighetsgenomgångar för att säkerställa att användare och deras åtkomsträttigheter hålls aktuella.
- System (servrar och virtuella servrar) ska skyddas mot skadlig kod, ha åtkomstkon-troll, loggfunktioner, backuprutiner och andra lämpliga säkerhetsåtgärder.
- Distansarbete skall möjliggöras med lämpliga säkerhetsåtgärder.
- Balco skall använda sig av relevant teknik och processer för att säkerställa att kommunikation både externt och inom koncernen sker på ett sådant sätt att verksamheten skyddas mot angrepp.
- Säkerhetsincidenter ska hanteras av personal med lämplig kompetens och mandat.
- Lämpliga IT-säkerhetsåtgärder ska definieras och tillämpas när avtal med leverantörer upprättas, dessa skall inkludera möjligheter till uppföljning.

3.3 Integritet och hantering av persondata

Balco skall följa tillämpbar lagstiftning i alla länder där verksamhet förekommer för att säker-ställa att anställdas och andra intressenters rättigheter i förhållande till personlig integritet inte kränks.

IT- och informationssäkerhets krav skall tillämpas för att säkerställa att lämpliga säkerhetsåtgärder vidtas för att skydda personuppgifter baserat på grad av känslighet. Processer och IT-tjänster ska utföras för att säkerställa överensstämmelse med lagstiftningen om uppgiftsskydd.

Förberedelser skall ske och lämpliga styrdokument liksom dokumenterade roller och ansvar ska finnas på plats så att Balco kan visa överensstämmelse med lokal lagstiftning liksom EU:s dataskyddsdirektiv (GDPR) vid en begäran om granskning från datainspektionen i syfte att undvika sanktioner och skador på Balcos varumärke.

- Det skall finnas en förteckning och klassificering av anställdas och andra intressenters persondata som behandlas inom Balco eller hos underleverantör på uppdrag av Balco oavsett på vilket media de lagras.
- Systemberoende ska dokumenteras för att säkerställa att det finns en tydlig uppdaterad vy över var personuppgifter behandlas, lagras och överförs.
- System som innehåller personuppgifter ska skyddas genom IT-säkerhetskontroller, inklusive men inte begränsat till åtkomstkontroll, backuprutiner och vid behov kryptering.
- Vid upphandling av IT-tjänster eller system där persondata kan behandlas skall principerna för privacy by design beaktas.
- Vid outsourcing ska det finnas en överenskommelse om hur personuppgifter hanteras och var de lagras.
- Personuppgiftsbiträdesavtal skall tecknas med samtliga underleverantörer som hanterar någon form av persondata på uppdrag av Balco.
- Återkommande riskbedömningar ska göras för att säkra korrigerande åtgärder kring områden där känsliga personuppgifter kan gå förlorade eller äventyras.
- IT-incidenthantering ska innehålla ett steg för att bedöma om en händelse är föremål för anmälan om överträdelse av uppgiftsförlust.

4 Roller och ansvar

- Denna policy är godkänd av styrelsen.
- VD är ytterst ansvarig för att Balco uppfyller förpliktelserna i denna policy genom att initiera upprättandet av nödvändiga styrdokument, utse roller (som kan kombineras) och ansvarsområden, processer och kontroller.
- VD ansvarar för att upprätthålla denna policy, för genomförande och övervakning av överensstämmelse.
- IT-chefen ansvarar för IT-säkerhet, inklusive att definiera krav och implementera dem.
- Systemägare ansvarar för dataskyddskraven och ska se till att nödvändiga IT-säkerhetskontroller genomförs i sina system.

5 Kriterier för efterlevnad

För att denna policy ska anses efterlevd ska följande kriterier vara uppfyllda:

- Policyn skall vara godkänd av styrelsen.
- Policyn skall vara kommunicerad och förankrad i ledningsgruppen.
- Policyn skall kommuniceras till all berörd personal årligen i samband med kvalitetsuppföljning.
- Policyn skall finnas lätt tillgänglig för all berörd personal.
- Policyn skall revideras årligen och uppdateras vid behov.

6 Övriga dokument

- IT-policy