CHECKLISTA INFORMATIONSSÄKERHET

BRANDVÄGGAR OCH UPPDATERADE OPERATIVSYSTEM ÄR VIKTIGA FÖR DIN INFORMATIONSSÄKERHET, MEN SKYDDAR INTE MOT ETT RISKFYLLT BETEENDE. DIN DIGITALA SÄKERHET HANDLAR OCKSÅ OM DITT BETEENDE OCH DIN MEDVETENHET OM RISKER.

- **Lämna aldrig din dator obevakad. Behöver du det, så logga alltid ut eller stäng av. Ditt konto är ditt ansvar.**
- **Se till att din dator, surfplatta och smartphone kräver inloggning (skärmlås) som automatiskt aktiveras.**
- **Sprid inte ut ditt lösenord genom att skriva upp det i närheten av din dator eller annan lättillgänglig plats.**
- **Låna inte ut ditt konto eller din utrustning som dator/mobiltelefon.**
- **Lämna aldrig ut ditt lösenord eller dina kontouppgifter till andra.**
- **Klicka inte på länkar och bilder som du inte vet var de kommer ifrån.**
- **Klicka aldrig OK utan att läsa vad du OK:ar till. Du kan råka installera virus eller annan skadlig programvara på din dator.**
- **Spara aldrig inloggningsuppgifter i din webbläsare eller i din dator.**
- **Ha alltid en uppdaterad version av antivirusprogram på alla dina enheter.**
- **Se till att alltid ha dina enheter uppdaterade med senaste versioner av programvara, operativsystem, mm.**
- **Hantera externa USB-minnen, minneskort och hårddiskar med försiktighet. De kan innehålla skadlig kod.**
- **Undvik att använda publika wifi. Enheter som är uppkopplade på samma wifi kan läsa trafiken samt du kan råka använda ett avsiktligt uppsatt falskt wifi som har till syfte att läsa din datatrafik.**

Earhart Academy utbildar ledare personal, specialister och vardagssurfare för att öka er digitala säkerhet.

Kurser: **www.earhart.academy**

Eller följ oss på LinkedIN där vi regelbundet delar videoklipp med tips och information.
Surfa säkert!

Verksamhetsstöd: **www.earhart.se**

EARHART
Business Protection Agency

INFORMATIONSSÄKERHET

Nyckeln till god informationssäkerhet är att veta vilken typ av informationstillgångar som finns och vem som behöver komma åt dem.

Informationssäkerhet är till stor del en fråga om hur system och arbetsrutiner organiseras och kontrolleras. Alla berörda i ett projekt eller en organisation behöver inte ha tillgång till all information i alla system.

Ett viktigt steg är att avgöra vilka roller som behöver tillgång till vilken typ av information och skapa behörighetstrappor och sedan ge dem åtkomst till rätt nivå.

Ett annat viktigt steg är att se till att projektet eller organisationen inte läcker information via tredjepartsleverantörer, dvs underleverantörer, partners och inhyrda konsulter.

Genomför bakgrundskontroller av leverantörer, samarbetsparter och resurser på nyckelfunktioner.

- Säkerställ att systemägarna känner till sitt ansvar och sina system, inklusive behörighetsrutinerna.
- Säkerställ att behörighetsrutiner för åtkomst av system och information upprätthålls.
- Säkerställ att behörigheter och åtkomster avslutas när avtal, inkl arbetskontrakt, upphör.
- Fastställ rutiner för informationssäker upphandling/inköp av nya system, tjänster, enheter, mm.
- Följ upp tredjepartsrelationerna regelbundet.
- Följ regelbundet upp klassning av information och tredjepartsleverantörer.
  Justera vid behov.
- Följ regelbundet upp risk- och sårbarhetsanalysen och justera rutiner vid behov.

CHECKLISTA SOCIALA MEDIER

TÄNK PÅ VAD DU LÄMNAR UT FÖR INFORMATION OM DIG SJÄLV OCH DIN FAMILJ. ÄR DU INTE AKTIV I SOCIALA MEDIER, HAR DU ETT OVANLIGT NAMN? SE TILL ATT ÄGA DIN IDENTITET I SOCIALA MEDIER ÄVEN OM DU VÄLJER ATT INTE VARA AKTIV. DET MINSKAR RISKEN FÖR ATT NÅGON SKA UTGE SIG FÖR ATT VARA DU.

Tänk på:

- **Ta del av användarvillkoren, vilken information lagras om dig och dina vänner. platsdata, vänlistor, historik eller access till kamera och mikrofon.**
- **Hur publik är du? Ofta är det du själv som måste ändra inställningar för vem som ska kunna se din profil och vad du publicerar.**
- **Dina digitala fotspår. Det är lätt att spåra en persons intressen och vanor via sociala medier. Information som kan utnyttjas av kriminella eller andra aktörer med oärliga avsikter för att skapa kontakt med dig.**
- **Bilder lämnar ut information om du inte aktivt har valt att ta bort bilddata. Tänk på att bakgrund, personer på bilden samt bilddata kan identifieras och användas av någon annan.**
- **Omvärldsbevaka din identitet. Se till att regelbundet söka efter din identitet så ingen använder den utan din vetskap.**
- **Säkra lösenord och säkra enheter. Aktivera tvåfaktorsautentisering för dina sociala medier.**
- **Var aktsam vid vänförfrågningar via sociala medier. Även om personen på bilden är någon du känner och flera av dina nuvarande vänner redan är vän med. Verifiera att det verkligen är rätt person bakom kontot. Risken för att det är en kapad identitet ökar om det är en publik person med viktig befattning.**

Falska nyheter, påståenden och inlägg i sociala medier kan avsiktligt ha publicerats för att påverka dig.

Var aktsam så du inte är med och bidrar till spridningen av desinformation som kan ha publicerats för att skada Sverige. Lär dig och din organisation mer.

EARHART
Business Protection Agency

Kurser: **www.earhart.academy**
Konsulttjänster: **www.earhart.se**

Risk - Sårbarhet - Hot - Säkerhet - Utredning - Beredskap - Kunskap

Informationssäkerhet, cyberhot, risk- och sårbarhetsanalys, hotbildsanalys, utredningar, bakgrundskontroller, utbildningar och krisövningar.

Välkommen till Earhart Business Protection Agency.

Det finns en rad åtgärder en verksamhet kan vidta för att säkerställa en god informationssäkerhet.

Earhart Business Protection Agency har konsulter med lång och gedigen erfarenhet på området. Vi har hjälpt företag, myndigheter, kommuner och länsstyrelser med att utarbeta olika åtgärder, och vi kan bland annat erbjuda följande:

- Hjälp att skapa och bygga en heltäckande styrdokumentation
- Utbildning för ledningsgruppen om system, lagstiftning och strategier.
- Utbildning för medarbetarna, särskilt rörande vardagsbeteende och sociala medier. (www.earhart.academy)
- Rådgivning till Ledning och styrelse.
- Analys av tredjepartsrelationer rörande informationssäkerhet.
- Cyber due diligence
- GAP-analyser för att uppnå ISO-standard 27001 och 27002

Kontakta oss för mer information
contact@earhart se
tel: 08-400 215 70

EARHART
Business Protection Agency

Verksamhetsstöd: www.earhart.se
Kurser: www.earhart.academy