Policy för anställda avseende digitala verktyg/ sociala medier/molntjänster

Gäller användning av företagets utrustning och datakommunikation & även för konsulter

Vi hanterar dagligen allt större mängder digital information, och det blir vanligare med digitala brott. Det finns därmed ökad risk att du förlorar utfört arbete eller att känslig information hamnar i orätta händer. Den största risken är många gånger vårt eget beteende. Att stanna upp och tänka till innan du klickar upp en länk eller e-postbilaga förhindrar de allra flesta virusattacker. När du ska hantera personuppgifter, tänk först efter om det verkligen är nödvändigt. Nästa steg är att tänka på är vilken typ av personuppgift det är och vilket skydd som krävs för att du ska hålla dig till GDPR. Personuppgifter får i många fall inte sparas längre än de används, kräver lagstöd & känsliga uppgifter måste hanteras i säkra system.

1. **Privat användning** av digital utrustning är tillåten i minsta mån men ska inte inkräkta på arbetstid och skall ske med gott omdöme. Det är till exempel inte tillåtet att besöka webbplatser som förknippas med pornografi, rasism eller nynazism, såvida det inte är professionellt motiverat. Privata mejl skall inte skickas med företagsadressen som avsändare och privata ljudfiler eller filmer skall inte lagras på företagets datorer eller lagringsytor. Några enstaka privata bilder är okej. Hur sociala medier används privat kan Anton utbildning inte styra över, men profession och den privata sfären tenderar idag att flytta ihop. Önskemål är att beakta detta, eftersom du som anställd ofta direkt förknippas och sammanlänkas med din arbetsplats/arbetsgivare.

2. **Upphovsrättsskyddat material** - Lagar och regler om upphovsrätt gäller även material som finns på internet. Det är inte tillåtet att använda information från internet på ett sätt som kränker upphovsrätten (t.ex. genom felaktig användning av bilder eller upp-/nedladdning av piratkopierat material).

3. **Hantering av konton och lösenord** - Lösenord är en allt viktigare del av vår digitala säkerhet och ska aldrig lämnas ut till någon annan och helst aldrig antecknas ner. Lösenord som används till Anton Utbildnings system får inte användas även privat, då det kraftigt ökar risken för intrång. Din arbetsdator/platta/telefon skall lösenordsskyddas och när den lämnas utan övervakning låsas eller stängas. Vid arbetsdagens slut skall du även alltid logga ur Google Drive/mail och andra arbetsrelaterade system! Glöm ej heller logga ur när du kopierat.

4. **Personuppgifter / känslig information** – Känsliga och integritetskänsliga personuppgifter skall alltid hanteras med försiktighet och endast då du har lagstöd för detta, dvs ej i mail utan i särskilda digitala system med stark autentisiering. Molntjänsten Google får endast användas med 2-stegs autentisiering och hantering av känslig information skall undvikas om möjligt eller raderas snarast möjligt. Tänk på att ha bildskärmen vänd så att obehöriga ej kan ta del av infon eller använd sekretessfilm. Var alltid säker innan du delar personuppgifter med annan än den berörda/berörde och dess vårdnadshavare.

5. **Installation av programvara** Om du installerar programvara som du varken fått via ramavtal eller enligt instruktion från Anton Utbildning måste du vara helt säker på att den är licensierad och inte innehåller skadlig kod. Om du är osäker, ta kontakt med IT-supporten. All lagrad information eller trafik kan under vissa förutsättningar komma att kontrolleras, exempelvis för att spåra hackerangrepp eller undersöka eventuella oegentligheter. Detta gäller även privat information eller användningshistorik som lagras i företagets utrustning och system.

6. **Skyldighet anmäla dataintrång / personuppgiftläckage** Om obehöriga kommit åt eller kan tänkas komma åt personuppgifter tex om USB-minne med personuppgifter tappats bort, om dator/telefon blivit stulen, om ngn hackat server, om ngn kommit åt dit lösenord och den vägen kan tänkas komma åt personuppgifter mm måste detta i enlighet med GDPR omgående anmälas till **dataskyddsombudet@antonskolan.com.**

Hantering av E-post & lagring i Google Drive

- **Skicka aldrig känsliga & integritetskänsliga personuppgifter** rörande religion, ras, genetik, sexliv, hälsa, fackförbund, politisk åskådning, lön, personnr eller extra känsliga personuppgifter såsom brott, personliga profiler, sociala förhållande och liknande via e-post.

- **Ett e-postmeddelande med personuppgifter får inte ligga kvar** i inkorgen eller annan mapp. När din behandling av personuppgifter är klar ska informationen antingen flyttas över till lämpligt system, säker lagring (om lagstöd) eller raderas.
  Den tid som en personuppgift lagras i e-posten ska begränsas till ett strikt minimum.

- I e-posten **får du inte behandla mail med känsliga personuppgifter som är känsliga eller sekretessbelagda**. Om känsliga eller sekretessbelagda personuppgifter inkommer kan du till inte vidarebefordra eller svara på mailet utan behandla på annat sätt och radera.

- **Använd e-post för att kommunicera, inte lagra.** En säkerhetsrensning är inställd för mail som lagrats i 3 månader (efter 2 månader flyttas de först till papperskorgen och efter ytterligare 1 mån raderas de helt). Detta är en extra säkerhet men rensning skall i första hand ske manuellt!

- **Om du måste använda e-post avseende personuppgifter**, se över om det går det att avidentifiera dessa!

- **Samma regler gäller vare sig du skickar e-post internt eller externt.**

- Nya medarbetare skall få hjälp att **ställa in 2-stegs autentisering i Google Drive**! Detta innebär 2-stegs autentisering när du loggar in på en ny enhet. Längre ner hittar du en guide.

- Kom ihåg att **logga ut** vid arbetsdagens slut!

- **Gallra och rensa din Google Drive ifrån personuppgifter vi inte har laglig grund för att spara.** Obs, vissa personuppgifter behöver vi spara långt efter att tex eleven slutat men de ska då lagras på annat sätt, se arkiveringsrutiner i ”personuppgiftesregistret”. Känsliga uppgifter i minsta möjliga mån och försök avidentifiera. Känslig uppgifter raderas efter behandling.

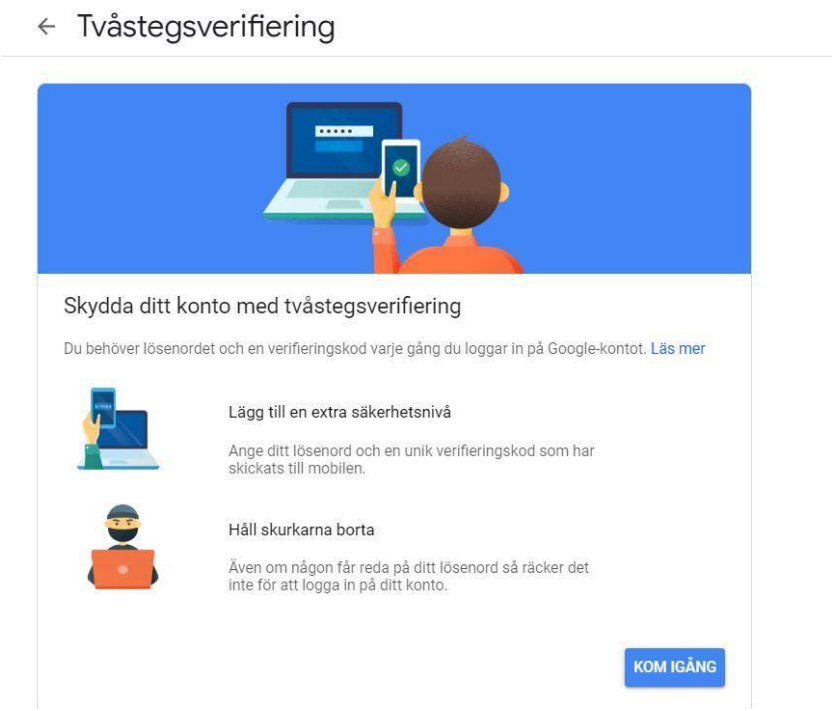
- **Vid delning av ett Google-dokument observera den andres behörighet till dokumentet!** Genom att klicka på avancerat kan du undvika att dokumentet med känsliga personuppgifter hamnar som direkt klickbart i personens mail. Se sid 4.

Som chef/ledare *ska du tillse att alla anställda på din enhet blir informerad om ovanstående*
Som kollega *hjälper du till genom att påminna om ovanstående punkter*
Som egen *ser du till att du följer ovanstående punkter*

Google Drive 2-faktors autentisering

Google-kontot är det vi använder i många avseenden, e-post, dokumentlagring, delning av mm. Att ställa in tvåfaktorsautentisering är obligatoriskt för din och företagets säkerhet. Nedan följer hur du går till väga. Hjälp kan du få av kollega, It-stöd eller Dataskyddsombudet.

Gå till https://www.google.com/landing/2step/ Där trycker du på ”Kom igång”.



Klicka ”Kom igång” ytterligare en gång. Du får sedan skriva in ditt vanliga lösenord till Google Drive(E-posten).

Du får sedan uppge om du vill autentisera med hjälp av sms eller via telefonsamtal, och till vilket telefonnummer. Google skickar sedan en kod till dig via mobilen som du får bekräfta, och du kan sedan välja ”Aktivera”. Sedan är tvåfaktorsautentisering aktiverat.

*Du kan komma att behöva **logga in** igen med ditt Google-konto på till exempel din mobil eller din dator. På sidan du då kommer till kan du se att tvåfaktorsautentisering är påslaget, och du kan också välja att aktivera fler alternativ om du till exempel skulle tappa bort din mobil eller om du skulle vara utomlands utan mobiltäckning. Ett alternativ är till exempel reservkoder som du kan skriva ut och använda i nödfall när du inte har tillgång till din mobil.*

*Du kan **avaktivera** tvåfaktorsautentisering genom att klicka på ”Inaktivera”. I samband med att du loggar in på en enhet kan du också välja att lägga till den som en ”Betrodd enhet”, då behöver du inte din mobil för att logga in på den. Det minskar dock säkerheten.*

Anton Utbildning

Delningsinställningar