PERSTORPS KOMMUN

Rutiner för IT-säkerhet

Perstorps kommun

RUTIN HANDBOK

Fastställt av: Säkerhetschef
Fastställt datum: 2024-09-18
Senast reviderat: 2024-09-18
För detta styrdokument ansvarar: Säkerhetschef
Dokumentet gäller för: Samtliga förvaltningar

1. Roller och ansvar

Alla medarbetare i kommunen ansvarar för att upprätthålla en god IT-säkerhet.

Chef ansvarar för att anställda har kännedom om Perstorps kommuns rutiner för IT-säkerhet.

Det är varje medarbetares ansvar att tillgodogöra sig kommunens rutiner för IT-säkerhet, hålla sig uppdaterad om förändringar och att följa rutinerna i det dagliga arbetet.

2. IT-utrustning

Vad är kommunens IT-utrustning?

Med IT-utrustning menas olika typer av utrustning såsom dator, laptop, mobil eller padda som anställd får tillgång till i sin roll som anställd.

Hur ska kommunens IT-utrustning hanteras?

Kommunens IT-utrustning ska hanteras på ett säkert och ansvarstagande sätt. Medarbetare ansvarar för att hantera, transportera och förvara IT-utrustning så att utomstående inte får tillgång till den.

Säker användning av IT-utrustning

Medarbetare ska inte använda kommunens IT-utrustning på ett sätt som utsätter organisationens information för risker.

Dator och liknande utrustning ska vara låsta när du inte har uppsikt över dem. Du låser din dator genom att trycka på Windows-knappen (knappen med flaggan) + L.

Var uppmärksam på vad du visar på din skärm och vem som kan se den. Detta gäller både inom kontoret och utanför, exempelvis om du arbetar under din pendling till jobbet. Om du hanterar sekretessbelagd information – använd gärna ett sekretessfilter på skärmen.

Klicka inte på länkar eller bilagor när du får mail eller SMS från okända avsändare. Är du osäker på om meddelandet innehåller något skadligt? Du kan alltid ringa EttIT Servicedesk – de kan öppna meddelandet åt dig och kontrollera om det innehåller skadligt innehåll.

Att ha Bluetooth och platstjänster påslaget gör din enhet synlig för andra aktörer, och kan öka risken för att för att någon försöker komma åt din data. Slå av dem när de inte behövs.

Anslut inte okända laddare eller USB-minnen till din dator. Dessa kan innehålla skadlig kod.

IT-utrustning som du får tillgång till i rollen som anställd ska inte användas för privat bruk.

3. Vilka programvaror får vi installera?

Medarbetare hämtar programvaror från Företagsportalen. I denna ligger program som EttIT har godkänt och kontrollerat.

Saknar du tillgång till ett program eller ser ett nytt behov? Vänd dig till din närmaste chef.

4. När du arbetar någon annanstans än på kontoret

Arbetar du hemifrån eller från annan ort? Kom ihåg att använda VPN-tjänst godkänd av EttIT.

Undvik att koppla upp dig på publika nätverk. Dela istället mobilt internet från din telefon.

När vi reser kan vi utsätta vår utrustning och vår information för andra risker än när vi jobbar på kontoret. Ska du resa i tjänsten? Var noga med att bara ta med dig den information och den utrustning du behöver. Läs inte över information till privata enheter som du har med dig på semesterresan.

5. Hantering av inloggningsuppgifter och lösenord

Vad är ett lösenord?

Ett lösenord är en fras eller antal tecken som du använder för att logga in i system eller appar.

Vi använder lösenord för att styra åtkomst till våra system och till vår information. Varje medarbetare ska endast ha tillgång till det som denne behöver i sin roll.

Hur ska lösenord väljas?

Det är bra att använda minst tolv tecken i ditt lösenord. Ditt lösenord är starkare om du inkluderar siffror eller specialtecken såsom utropstecken eller frågetecken. Det är även bra att använda en ”nonsens-fras”, en mening som är lätt för dig att komma ihåg men svår för andra att gissa sig till.

Undvik att använda din födelsedag eller ditt namn som lösenord. Undvik även vanliga kombinationer såsom ”lösenord123”. Dessa är enklare att gissa sig till.

Hur ska lösenord hanteras?

Du ska inte ge ut ditt lösenord till någon annan. Du är ansvarig för att hålla dina lösenord skyddade och hemliga. Undvik att skriva ner dina lösenord och att spara dem i webbläsaren för automatisk inloggning. Ju känsligare data som finns i systemet, desto viktigare är det att du hanterar dina lösenord så att ingen otillbörlig kan komma in i systemet.

Om du misstänker att någon som inte bör ha tillgång till kommunens data har fått reda på ditt lösenord, byt det så snabbt som möjligt. Du ska även rapportera incidenten till EttIT ServiceDesk.

Genom att hålla dina lösenord starka och hemliga förhindrar du att kommunens information sprids till fel aktörer. Du hjälper även till att garantera att bara rätt personer har åtkomst till att göra ändringar i våra verksamhetssystem.

Lösenord bör bytas regelbundet.