IT sikkerhedshåndbog

for NEG Elever

Formål

Formålet med denne håndbog er, at skabe opmærksomhed på IT-sikkerhed, og hvorfor det er vigtigt for NEG at have en IT-sikkerhedspolitik.

Sikkerhedstrusler mod virksomheder og privat personer, har aldrig været større. Flere og flere oplever angreb på virksomhedens IT-systemer og data.

IT sikkerhed er i høj grad afhængig af, at brugerne udviser omhu og naturlig skepsis i den daglige brug af IT.

God læselyst

> *"Mennesker repræsenterer det svageste led i IT-sikkerhed og er ofte ansvarlig for svigt i sikkerhedssystemer".*
>
> - Bruce Schneier, krypterings ekspert

> *Virksomheder bruger millioner af dollars på firewalls, kryptering og sikre adgangs enheder, og det er spild af penge, fordi ingen af disse foranstaltninger sikrer det svageste led i IT-sikkerheden".*
>
> - Kevin Mitnick, berømt hacker

Gode råd omkring et sikkert IT miljø på NEG

Følgende afsnit indeholder sikkerhedsråd, der skal styrke IT-sikkerheden på NEG

- Ledelsen skaber opmærksomhed om brug af IT-sikkerhed
- Der udarbejdes en IT-sikkerhedspolitik
- Brugere holdes opdateret om tiltag
- Styresystemer på pc'ere skal opdateres regelmæssigt
- Software skal ligeledes holdes opdateret

Din egen pc

Hvis du skal ud og købe en pc, der skal bruges på skolens netværk, så vær opmærksom på, at styresystemet **Windows 10 S og Windows 11 S** ikke er anvendeligt, hvis der skal installeres software på enheden.

Beskyt dig og din computer med en stærk adgangskode

En stærk adgangskode indeholder:

- Mindst 8 karakterer
- Udskift bogstaver med tal eller tegn f.eks a med @ og o med 0 (nul)
- Bland store og små bogstaver

Brug ikke

- En adgangskode der er nem at gætte, som f.eks. navn på børn, ægtefælde, hund eller lignende
- Ord der kan slås op i ordbogen
- Din eller dine nærmeste's fødselsdage

Eks. Password123 har 11 tegn med store og små bogstaver og tal. Problemet med Password123 er, at det ikke opfylder kravet til en stærk adgangskode. Brug i stedet: P@$$w0rd123

Vigtigheden af stærke adgangskoder

Når der anvendes mindre stærke adgangskoder, er det meget nemmere for hackere at knække koden.

Hackere bruger ofte værktøjer som Dictionary attack.

Din adgangskode og dit brugernavn er personligt, del ikke med andre

Alle brugere, der har adgang til NEGs data, er ansvarlig for deres eget brugernavn og adgangskode. Det er personligt og må ikke deles med andre.

Ligeledes må du ikke give tilladelse til, at andre bruger dit login for at tilegne sig adgang til NEGs data. Og du må naturligvis heller ikke bruge andres login og adgangskode.

Hvis login og adgangskoder deles mellem to eller flere brugere, kan de aktiviteter, der udføres med dette bruger-id ikke spores tilbage til den korrekte person.

Brug af internet

Når du bruger internettet fra NEGs netværk, repræsenterer du virksomheden, da elektronisk kommunikation efterlader spor (cookies).

Det er vigtigt at du tænker over din adfærd, når du færdes på nettet. Hvis du modtager pop-up vinduer fra hjemmesider, chatbeskeder, eller andre anmodninger om bruger-id og adgangskode, bør du være særlig opmærksom. Det kan være et forsøg på, at få adgang til dit system.

Kig efter i HTTPS i URL'en eller en lille lås i højre hjørne af din browser. Det indikerer, at de oplysninger du sender via din browser er krypteret.

Brugernes måde at benytte internettet, er afgørende for sikkerheden

En uhensigtsmæssig anvendelse af internettet, kan skabe potentielt risiko for hele virksomheden og medføre betydelige omkostninger.

Problemer med sikkerheden kan opstå, når en bruger bevidst eller ubevidst benytter ulovlige, offensive, farlige eller ikke forretningsrelaterede internetsider og programmer.

Er noget for godt til at være sandt, så er det formentlig heller ikke sandt.

Vær opmærksom på hvad du downloader

Vær påpasselig med, hvilke eksekverbare filer eller programfiler du henter fra internettet. Undtagen hvis ansøgningen er fra en kendt og pålidelig kilde, samt den digitale signatur er blevet kontrolleret uden problemer.

Installer kun software fra producenter og leverandører du har tillid til. Spørg evt. IT.

Download eller opbevaring af spil, musik eller lignende indhold, der ikke er korrekt licenseret eller materiale, der er beskyttet af ophavsret, er ikke tilladt på skolens udstyr.

Det er ikke tilladt at installere software på NEGs udstyr.

Brug ikke peer-to-peer-klient-software, såsom Bittorrent, da den type software kan være en skjult adgang for hackere.

Udvis forsigtighed ved brug af e-mail

Vi kommunikerer i stigende grad via e-mail. E-mail bør betragtes som et åbent postkort, der let kan læses af alle der håndterer e-mailen fra afsender til modtager. Hackere kan nemt opsnappe informationer under forsendelsen.

Personlige data må ikke sendes ukrypteret brug i stedet e-boks, hvis du skal sende personfølsomme oplysninger videre.

E-mail kan krypteres, hvilket svarer til at sende det åbne postkort i en lukket kuvert. E-mailen kan ikke læses, før den endelige modtager åbner kuverten.

- Vær opmærksom, når du modtager e-mails med vedhæftede filer og links
- Vær opmærksom på, at virus kan komme fra en ven eller familie
- Tjek om mailen indeholder åbenlyse stavefejl, forkert tekst el. lign.
- Udvis forsigtighed, når du udleverer din e-mail. Du kan risikere SPAM
- Pas på falske emails (phishing). Klik aldrig på link eller vedhæftede dokumenter i emails, som du ikke er 100% sikker på kommer fra en troværdig kilde – og husk at it-kriminelle ofte bruger Skat, banker, postvæsenet m.v. som afsender på deres falske emails.

Det er vigtigt, at du ikke accepterer nogen former for hjælp, medmindre du selv har bedt om det.

Acceptér aldrig tilbud om gratis rådgivning, besvar ikke spørgeskemaer eller undersøgelser fra upålidelige kilder. Brug ikke gratis sikkerhedsprogrammer, medmindre den specifikke leverandør er godkendt af IT.

Oplys aldrig din kode, Nemid eller dit konto nr. til andre.

WIFI trådløst netværk

NEG tilbyder trådløst netværk for ansatte og elever.

"NEG" – sikret netværk med login og adgangskode

"NEG-guest" – åbent net hvor alle kan komme på og dermed en usikker forbindelse, hvor man ikke bør sende personlige eller økonomiske oplysninger gennem.

Mobiltelefoner

Da mobiltelefoner i dag kan næsten det samme som en pc, bør du sikre din telefon.

Telefonen bør være beskyttet med låseskærm, hvor koden består af mindst 6 tal.

Yderligere bør telefonen være forsynet med simkode på 4 tegn.

Del ikke gadgets på mobiltelefonen, det er en øget sikkerhedsrisiko.

Klik aldrig på et link der sendes i en SMS.

Anvendelse af skolens pc'ere

Når du låner skolens udstyr, skal det behandles ordentligt, misligholdelse/mishandling kan medføre at brugeren stilles til ansvar for reparationsudgifter.

Installation af software, spil m.v. må ikke foretages.

Der må ikke spises og drikkes ved udstyret.

Skolens udstyr er registreret på skolens netværk.

Tyveri af udstyr straffes med…

Ansvar ved mistanke på sikkerhedsbrud

Ved mistanke om sikkerhedsbrud skal skolens IT-sikkerhedschef informeres.

Hvad gør NEG for at mindske risikoen for sikkerhedsbrud

Alle brugere skal anvende eget login og password

Harddiske i NEGs udstyr krypteres

Firewall installeres på alle pc'ere tilhørende NEG.

Adgang til netværksdrev vurderes pr. bruger/gruppe, og tildeles via sikkerhedsgrupper

Der logges adfærd fra alle systemer og tjenester

Rettigheder til installation fratages elever som led i Ministeriets nye sikkerhedsregler.

Adgang til netværksdrev, print m.v. kan kun etableres via login og password

Ordforklaringer

Antivirus – Program der sikrer enheden mod virus

Bittorrent – Program hvor brugere deler filer

Browser – Program til visning af hjemmesider. Internet Explorer, Firefox og Goodle Chrome

Cookie – Indsamling af indformationer fra de enheder der har besøgt en hjemmeside

Dictionary attack – Hacker bruger et program med ord fra en ordbog til at bryde adgangskoder

Firewall – Adskillelse af virksomhedens netværk mod internettet, og sikring af kommunikation og data der sendes på netværket

Hacker – Person der finder og udnytter svagheder i sikkerheden i et computersystem eller i et netværk

Malware – Ondsindet program, hvis formål er at gøre skade på computere og netværk

Phishing-angreb – Svindlere forsøger at franarre godtroende internetbrugere fortrolige oplysninger

Ransomware – Digital form for gidseltagning. Hackeren krypterer brugernes filer og dokumenter, så de ikke kan tilgås. Hackerne kræver løsepenge for at frigive dem.

SPAM – Betegnelse for uønskede reklamer, der sendes via mail eller i nyhedsgrupper

Spyware – Program der usynligt installerer sig på brugerens computer med det formål, at samle informationer og spore aktiviteter

VPN – Betyder Virtuel Privat Netværk. En forbindelse der typisk oprettes over internettet, så man kan arbejde på farten, og tilgå virksomhedens netværk på en sikker og krypteret forbindelse.

WIFI – Trådløst netværk