Informationssikkerhedspolitik for

Nordjyllands Landbrugsskole

Version	Dato	Ændret af	Godkendt af
1.0			

Indhold

Formål

Informationssikkerhedspolitik beskriver vigtigheden af arbejdet med informationssikkerhed i virksomheden og fastlægger vores ambitionsniveau herfor. Informationssikkerhedspolitikken indeholder derfor de overordnede sikkerhedsmålsætninger og danner grundlag for udformning af virksomhedens informationssikkerhedshåndbog, der forstås som fællesbetegnelsen af informationssikkerhedspolitikken med de underliggende retningslinjer og forretningsgange.

Informationssikkerhedshåndbogen findes i bilag 1.

Informationssikkerhedspolitikken er en vigtig del af virksomhedens sikkerhedshåndbog og beskriver det ledelsesgodkendte niveau for sikkerhed. Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i virksomhedens organisation og virke. De retningslinjer, der udformes for at understøtte informationssikkerhedspolitikkens hovedmålssætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til informationssikkerhed i det daglige arbejde.

Vi ser ikke kun et højt sikkerhedsniveau som et krav for at kunne overholde lov- og myndighedskrav, men også som et kvalitetselement for at kunne tilbyde en sikker service for vores samarbejdspartnere.

Informationssikkerhed er derfor en nøgleværdi hos os, og den vil være en naturlig del af vores it-aktiviteter.

Omfang

Informationssikkerhedspolitikken er gældende for alle vores medarbejdere.
Alle leverandører og samarbejdspartnere, som har fysisk eller logisk adgang til vores systemer, data og informationer skal gøres bekendt med politikken og følge den.

Informationssikkerhedspolitikken dækker alle tekniske og administrative forhold, der har direkte eller indirekte indflydelse på drift og brug af vores it-systemer.

Hovedmålsætninger og sikkerhedsniveau

Sikkerhedsmålsætning:
"Vi vil have et tilstrækkeligt informationssikkerhedsniveau for alle ansatte, elever, samarbejdspartnere og for anvendelsen af it-ressourcer, såsom it-systemer, hardware samt elektroniske datamedier på Nordjyllands Landbrugsskole"

Et tilstrækkeligt informationssikkerhedsniveau opnås igennem sikringsforanstaltninger, der sikrer:
1. Fortrolighed, integritet og tilgængelighed af systemer og data i forhold til den it-risikovurdering, der er fastsat for det enkelte system/data.
2. Beskyttelse af it-aktiver, medarbejdernes kompetencer, organisationens image og informationer/data i vores varetægt.

For at fastholde det tilstrækkelige sikkerhedsniveau skal følgende overholdes:

- Der skal forefindes retningslinjer og forretningsgange, som sikrer, at informationssikkerhed er en integreret del af vores drift og daglige arbejde.
- Vi skal igennem kontrakt- og leverandørstyring sikre, at brugen af eksterne konsulenter, samarbejdspartnere og leverandører ikke udhuler informationssikkerhedsniveauet.
- Vi skal følge op på informationssikkerheden ved løbende vedligehold og optimering af informationssikkerhedspolitikken og de dertilhørende retningslinjer og forretningsgange. Målet er at sikre en struktureret og kontinuerlig forbedringsproces.

Organisation og ansvar

Sikkerhedsmålsætning:
"Alle medarbejdere har ansvar for informationssikkerheden. De er bekendte med og efterlever vores Informationssikkerhedspolitik, Persondatapolitik og regler angivet i Personalehåndbog for IT og Persondata"

Planlægning, implementering og kontrol af informationssikkerhed er defineret af ledelsen.
IT-afdeling og administration er ansvarlig for implementering og vedligeholdelse af informationssikkerheden og er ansvarlig for opfølgning på sikkerhedshændelser.

Informationssikkerhedspolitikken revurderes og godkendes i forbindelse med eventuelle situationer, der tilsiger det. Forstanderen er ansvarlig for at arbejde med informationssikkerhed på et strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger. Ledere og medarbejdere er ansvarlige for at efterleve retningslinjer og procedurer for sikkerhed i det daglige arbejde.

Den nødvendige viden og kompetence omkring informationssikkerhed kommunikeres til alle medarbejdere, og der bliver løbende arbejdet med holdninger og viden omkring informationssikkerhed. Ledelsen er ansvarlig for, at informationssikkerheden overholdes.

Klassifikation

For at sikre at vores systemer og data har det rigtige sikkerhedsniveau, er disse identificeret og klassificeret i særskilt dokument "Risikoanalyse for IT-aktiver", som indgår i den samlede. Der er udarbejdet en fortegnelse over alle væsentlige it-aktiver, både hardware og software.
Der er angivet ansvarlige ejere for alle kritiske it-aktiver.
Data og systemer er klassificeret i forhold til tilgængelighed og til sikkerhed (fortrolighed og datas integritet)

Tilgængelighed af data og systemer inddeles i følgende kategorier:

- svært høj, høj, middel, lav, ubetydelig

Integritet for data og systemer inddeles i følgende kategorier:

- svært høj, høj, middel, lav, ubetydelig

Konfidentialitet for data og systemer inddeles i følgende kategorier:

- svært høj, høj, middel, lav, ubetydelig

Overtrædelse af informationssikkerhedspolitikken

Alle medarbejdere er forpligtet til at efterleve den til enhver tid gældende informationssikkerhedspolitik med tilhørende retningslinjer, forretningsgange og relaterede bilag, herunder Persondatapolitik på Nordjyllands Landbrugsskole samt regler angivet i Personalehåndbog for IT og Persondata på Nordjyllands Landbrugsskole. En overtrædelse kan, efter omstændighederne, medføre sanktioner.
Hvis en medarbejder er vidende om, at informationssikkerhedspolitikken overtrædes, skal det meddeles til ledelsen hurtigst muligt.

Hvis der opstår situationer, hvor kravene i informationssikkerhedspolitikken ikke kan efterleves, skal der skriftligt anmodes om dispensation af ledelsen. Eventuelle afvigelser fra kravene skal dokumenteres, og der skal indføres alternative sikringsforanstaltninger.

Bilag 1 - Informationssikkerhedshåndbogen

Dette afsnit beskriver procedurer og kontroller for Nordjyllands Landbrugsskoles informationssikkerhed.

1. Risikovurdering og -håndtering

Der foretages årligt en risikovurdering på virksomhedens IT-aktiver med hensyntagen til trusler, sårbarheder, sandsynlighed og konsekvens. Baseret på risikovurderingen implementeres der tiltag til at reducere højrisikoområder og diverse beredskabsplaner, backupstrategier og sikkerhedsforanstaltninger justeres iht. risikovurderingen.

2. Overordnede retningslinjer

2.1. Informationssikkerhedsstrategi

2.1.1. Formulering af en informationsinformationssikkerhedspolitik

Nordjyllands Landbrugsskole har vedtaget denne politik om informationssikkerhed, som kommunikeres til medarbejdere og relevante eksterne parter.

2.1.2. Løbende vedligeholdelse

Informationssikkerhedspolitikken gennemgås en gang årligt, samt opdateres efter behov

3. Organisering af informationssikkerhed

3.1. Interne organisatoriske forhold

3.1.1. Roller og ansvarsområder for informationssikkerhed

Ansvar for informationssikkerhed er defineret og fordelt. Forstander er ansvarlig for den generelle informationssikkerhed, IT-afdelingen er ansvarlig for informationsprocesser og IT-aktiver

3.1.2. Funktionsadskillelse

Det er så vidt muligt sikret, at ingen enkeltperson kan få adgang til, ændre eller bruge aktiver uden autorisation eller uden at det opdages. Hvis effektiv funktionsadskillelse er umuligt grundet organisationens størrelse, er der implementeret kompenserende kontroller i form af overvågning og tilsyn fra ledelsens side.

3.1.3. Kontakt med myndigheder

I tilfælde af at der er behov for at kontakte myndigheder i forbindelse med brud på sikkerheden er IT-afdeling eller administration ansvarlig herfor.

3.1.4. Kontakt med særlige interessegrupper

For at opretholde et tilfredsstillende vidensniveau vedrørende it-sikkerhedsinformation er IT-afdeling og administration medlem af erfa-gruppe i IT-center Nord, og har adgang til konsulenthjælp samme sted.

3.2. Mobilt udstyr og fjernarbejdspladser

3.2.1. Politik for mobilt udstyr

Procedure for registrering af mobilt udstyr, herunder bærbar PC, tablet og mobiltelefon:

> Alle PC'ere udleveret af Nordjyllands Landbrugsskole er entydigt registreret

Krav til fysisk beskyttelse:

> Mobilt udstyr må ikke efterlades uden opsyn på offentlige steder, møderum eller andre ubeskyttede områder. Mobilt udstyr skal beskyttes mod tyveri og bør ikke efterlades i transportmidler, hotelværelser, konferencecentre og mødelokaler.

Adgangsstyring:

> Alle brugere identificeres ved UNI-login, og systemadgange rettighedsstyres efter medarbejderens funktion

Malwarebeskyttelse:

> Der er installeret F-Secure antivirusprogram på alle PC'ere udleveret af Nordjyllands Landbrugsskole

Deaktivering, sletning eller spærring: Ved ansættelsesophør deaktiveres/slettes alle systemadgange, herunder adgang til elevadministrationssystem, Navision, Office 365, Uni-login, Medarbejder-nemID, VEU, Efteruddannelse.dk, SU, banksystemer mm. Forstander, administration og IT-afdeling er ansvarlig herfor

Backup: Der sker lokal back-up af fælles-mapper på Office 365, der sker **ikke** back-up af data gemt på medarbejdernes egen One-drive-platform

Privatejet mobilt udstyr:

Sikkerhedsforanstaltninger til at beskytte adskillelse af privat og arbejdsrelateret brug af udstyr:

> Privat mobilt udstyr, der benyttes til at tilgå skolens systemer, skal sikres af adgangskode og benyttes med samme disciplin, som udstyr, der er udleveret af Nordjyllands Landbrugsskole
>
> Adgang til forretningsinformationer via privat ejet mobilt udstyr er betinget af en accept af medarbejderens forpligtelser vedrørende fysisk beskyttelse jf. Personalehåndbog for IT og Persondata på Nordjyllands Landbrugsskole. Der skal altid ske softwareopdatering straks efter, at disse er tilgængelige. Medarbejderen giver afkald på ejerskab af forretningsdata, og giver tilladelse til, at organisationen sletter data på udstyret i tilfælde af tyveri, tab eller skade på udstyret, eller når brugeren ikke længere er autoriseret til at have adgang til forretningsinformationer.

3.2.2. Politik for fjernarbejdspladser
Regler for fjernarbejdspladsens fysiske sikkerhed, miljø, kommunikationssikkerhed, trussel om uautoriseret adgang for andre personer i boligen, malwarebeskyttelse og procedure for back-up er de samme, som angivet for den lokale arbejdsplads, jf. beskrivelse i IT-håndbog og Persondatapolitik for Nordjyllands Landbrugsskole

4. Medarbejdersikkerhed

4.1. Sikkerhedsprocedure før ansættelse

4.1.1. Screening
Medarbejdere bliver før deres ansættelse screenet på relevante områder iht. den pågældende jobbeskrivelse

4.1.2. Ansættelsesvilkår og -betingelser
Alle medarbejdere underskriver et tillæg til ansættelseskontrakt vedr. persondatasikkerhed for medarbejderen. I forbindelse med dette tillæg kvitterer medarbejderen for at have modtaget og forstået

1. Personalehåndbog IT og persondata for Nordjyllands Landbrugsskole
2. Persondatapolitik for Nordjyllands Landbrugsskole
3. Informationssikkerhedspolitik for Nordjyllands Landbrugsskole

Her er det klart defineret, hvilket ansvar medarbejderen har i forbindelse med informationssikkerhed.

4.2. Under ansættelsen

4.2.1. Ansvar
Ledelsen kræver, at alle medarbejdere fastholder informationssikkerhed. Medarbejdere er grundigt orienteret om deres roller og ansvarsområder for informationssikkerhed via Personalehåndbog IT og persondata, Persondatapolitik for Nordjyllands Landbrugsskole samt Informationssikkerhedspolitik for Nordjyllands Landbrugsskole

Hvis en medarbejder bliver bekendt med, at informationssikkerhedspolitikken ikke overholdes skal dette rapporteres til forstanderen – der arbejdes på en anonym elektronisk løsning

4.2.2. Uddannelse, træning og oplysning om informationssikkerhed
Medarbejderne bliver løbende trænet og holdt ajour med informationssikkerhedspolitikken og procedurer i det omfang, det er relevant for deres jobfunktion, herunder deltagelse i CyberPilots elektroniske awareness-træning

4.2.3. Sanktioner
Hvis en medarbejder ikke overholder informationssikkerhedspolitikken, kan der være sanktioner forbundet hermed

4.3. Ansættelsens ophør eller ændring

4.3.1. Ansvar ved ansættelsens ophørs
Forstanderen har ansvaret for at kommunikere eventuelle fratrædelser eller ændringer i ansættelsesforhold til andre relevante afdelinger via afdelingsledermøder eller fælles elektronisk platform

4.3.2. Inddragelse af rettigheder
IT-afdelingen og administrationen har på foranledning af forstanderen ansvaret for at nedlukke brugere ved ansættelsesophør eller justere rettigheder ved ændringer i ansættelsesforholdet.

5. Styring af informationsrelaterede aktiver

5.1. Identifikation af og ansvar for informationsrelaterede aktiver

5.1.1. Fortegnelse over informationsaktiver
Nordjyllands Landbrugsskole har udarbejdet en fortegnelse over IT-aktiver og deres betydning som gennemgås årligt og opdateres løbende.

5.1.2. Ejerskab
Når et IT-aktiv oprettes, bliver dette tildelt en ejer/afdeling, som har ansvaret for korrekt styring af aktivet i hele dets livscyklus. Ejeren har ansvaret for at aktivet opføres i fortegnelsen omtalt ovenfor og at det klassificeres og beskyttes på behørig vis. Ejeren definerer og gennemgår regelmæssigt adgangsbegrænsninger og klassifikationer for aktivet, under hensyntagen til gældende politikker for adgangsstyring. Det er ejerens ansvar, at aktivet håndteres korrekt, når det slettes eller destrueres.

5.1.3. Accepteret brug af aktiver
Der er klare regler for accepteret brug af virksomhedens IT-aktiver relateret til informationssikkerheden.

5.1.4. Tilbagelevering af aktiver
Alle medarbejdere og eksterne brugere skal aflevere alle virksomhedens aktiver i deres besiddelse tilbage, når deres ansættelse, kontrakt eller aftale ophører.

Ved ansættelsens ophør udleveres en liste over IT-aktiver, som medarbejderen skal aflevere til IT-afdelingen.

Op til ansættelsens ophør kan der holdes ekstra øje med medarbejderens aktiviteter, således at det kan kontrolleres, at medarbejderen ikke foretager uautoriseret kopiering af relevant information.

5.2. Klassifikation af informationer

5.2.1. Klassifikation
Informationer er klassificeret af ejeren, baseret på eventuelle lovmæssige krav, værdi og efter hvor kritisk og følsom informationen er i forhold til uautoriseret offentliggørelse eller ændring. Beskyttelsesniveauet for it-aktiverne er baseret på en analyse af behovet for fortrolighed, integritet og tilgængelighed. Klassifikationen opdateres løbende af aktivejeren.

5.2.2. Mærkning og håndtering af informationer
Alle fortrolige informationer er mærket.

5.3. Mediehåndtering

5.3.1 Styring af flytbare medier
Inden genanvendelige medier, fx USB-stik, flyttes fra organisationen, skal indhold, der ikke længere er brug for, slettes uopretteligt. Alle medier skal opbevares sikkert og hvis datafortrolighed eller integritet er vigtigere end normalt, skal der anvendes kryptering til at beskytte data på mediet.

Generelt bør anvendelse af flytbare medier begrænses som meget som muligt.

5.3.2 Bortskaffelse af medier
Når der ikke længere er behov for et medie, skal det bortskaffes på forsvarlig vis. Fysiske enheder f.eks. harddisk og usb-stik destrueres fysisk

5.3.3 Transport af fysiske medier
Der anvendes pålidelige transportører af medier

6. Adgangsstyring

6.1. De forretningsmæssige krav til adgangsstyring

6.1.1. Politik for adgangsstyring
Medarbejdere og eksterne partner får kun adgang til informationer på need to know-basis dvs. at der kun bliver tildelt de adgange til information, som vedkommende har behov for, for at kunne udføre sine arbejdsopgaver. Dette afgøres af brugerens nærmeste leder.

Medarbejdere og eksterne partnere får kun adgang til det IT-udstyr, applikationer og lokaler, som vedkommende har behov for, for at kunne udføre sine opgaver. Dette afgøres af brugerens nærmeste leder.

6.1.2 Adgang til netværk og netværkstjenester
Der kan opnås adgang til følgende netværk: S-net samt Gæstenærtværk. Sidstnævnte giver udelukkende adgang til internet.

Brugere skal autoriseres af IT-afdeling, før de får adgang til netværket.

Adgangen til netværksforbindelser er beskyttet af brugerlog

Netværket kan tilgås via LAN, WiFi og VPN

Der skal tastes brugernavn og adgangskode for at opnå adgang til netværk

Brugen af netværkstjenester overvåges.

6.2. Administration af brugeradgang

6.2.1. Brugerregistrering og afmelding
Alle brugere har deres eget unikke bruger-ID. Fællesbrugere anvendes kun, hvis det er nødvendigt af forretnings- eller driftsmæssige årsager.

Nedlagte bruger-ID'er bliver regelmæssigt slettet (mindst 1 gang årligt). Der er sat udløbsdato på elevers bruger-ID, således at disse slettes 5 år efter gennemførsel af 2. hovedforløb

Gamle bruger-ID'er må ikke tildeles nye brugere.

6.2.2. Tildeling af brugeradgange
Før en bruger tildeles adgang til informationssystemer, skal dette godkendes af ejeren af informationssystemet i samarbejde med brugerens nærmeste leder.

6.2.3 Styring af privilegerede adgangsrettigheder
Privilegerede adgangsrettigheder til operativsystemer, databaser og applikationer er begrænset til de brugere, som har et arbejdsrelateret behov herfor.

Generiske administrator-ID'er er kun kendt af få personer og særligt beskyttet med hyppig ændring af adgangskoder.

6.2.4 Styring af brugeres adgangskoder
Medarbejderen må ikke dele sin autentifikationsinformation med andre.

Medarbejderen skal ændre sin adgangskode første gang der logges ind.

Medarbejderens identitet bliver verificeret før der gives ny, ændret eller midlertidige adgangskoder

Midlertidige adgangskoder skal gives til brugere på forsvarlig vis, dvs. ikke ubeskyttede (klar tekst) mailbeskeder og lignende

Midlertidige adgangskoder må ikke være noget, man kan gætte sig til

Forudbestemte adgangskoder fra leverandører ændres efter installation af systemer eller software.

6.2.5 Gennemgang af brugernes adgangsrettigheder
Brugeradgangsrettigheder bliver gennemgået årligt

6.2.6 Inddragelse eller justering af adgangsrettigheder
Når en medarbejder stopper bliver vedkommendes logiske og fysiske adgang inddraget. Forstander oplyser IT-afdeling og administration om fratrædelser og IT-afdelingen og administration er derefter ansvarlig for at lukke diverse brugeradgange og skifte passwords til eventuelle fælles brugere.

Når en medarbejder får en ny stilling eller afgiver/fratages specifikke arbejdsopgaver, oplyser forstander dette til IT-afdelingen som har ansvaret for at tilpasse vedkommendes logiske og fysiske adgange til informationsaktiver.

6.3 Brugernes ansvar

6.3.1 Brug af hemmelig ID og password
Brugere må ikke udlevere deres ID eller password til andre.

Brugere må ikke registrere deres ID eller password på papir, i software-filer eller håndholdt udstyr, med mindre der er tale om en sikker password vault.

Brugeren skal ændre deres password ved mistanke om kompromittering.

Brugeren skal vælge password der er:

- nemme for dem at huske
- ikke kan gættes eller udledes ved hjælp af personoplysninger, fx navne, telefonnumre, fødselsdatoer
- Ikke er sårbare over for ordbogsangreb (dvs. ikke består af ord, som er indeholdt i ordbøger)
- Ikke indeholder flere på hinanden følgende ens karakterer, som kun består af enten tal eller bogstaver
- Brugeren skal undgå at anvende samme password til private og arbejdsmæssige formål.

6.4. Styring af system- og applikationsadgang

6.4.1. Begrænset adgang til informationer
Systemer og applikationer er indrettet således, at det er muligt at give forskellige brugere adgang til forskellige funktioner. Det kan ligeledes styres, hvilke data, der kan gøres tilgængelige for en bestemt bruger eller brugergrupper. Det kan styres, hvilke brugere, der har læse-, skrive-, slette- og execute-rettigheder.

Følsomme applikationer og informationer er isoleret fra andre systemer.

6.4.2. Procedure for sikker log-on
Der logges på skolens administrative systemer og Office 365 via single sign on (Uni-login). Ved øvrige systemer bruges Nem-ID eller selvskabt bruger-id/adgangskode

Log-on skærmen viser ikke hjælpemeddelelser, som ville kunne misbruges af en uautoriseret bruger.

Log-on-oplysninger valideres først, når alle inputdata er registreret, så hvis der opstår en fejl ved log-on vises det ikke, om det er brugernavnet eller adgangskoden mv., der er forkert.

Passwordet som indtastes vises som * og ikke i klar tekst og transmitteres ikke som klar tekst for at undgå, at de opsnappes af sniffer-programmer.

Inaktive sessioner afsluttes i administrationen efter 15 minutter med inaktivitet.

6.4.3 System for administration af adgangskoder
Systemet for administration af adgangskoder sikrer

- brugen af unikke bruger-ID'er og adgangskoder
- at adgangskoderne af høj kvalitet
- at brugeren skifter adgangskode ved første log-on
- at adgangskoden skiftes hver 100 dag
- at tidligere anvendte adgangskoder ikke kan genbruges
- at adgangskoder ikke vises på skærmen under indtastning
- at adgangskoder transmitteres i krypteret form

6.4.4 Brug af privilegerede systemprogrammer
Brugen af systemprogrammer, som kan omgå system- og applikationskontroller er begrænset til IT-afdelingen

7. Kryptografi

7.1 Kryptografiske kontroller

7.1.1 Politik for anvendelse af kryptografi
Brugen af kryptografi i organisationen sker ved brug af E-boks ved personfølsomme data.

7.1.2 Administration af nøgler
Krypteringsnøgler administreres af IT-center Nord

8. Fysisk sikring og miljøsikring

8.1 Fysisk sikring

8.1.1 Fysisk perimetersikring
Organisationens områder er kontrolleret via kameraovervågning

Ydertag, mure og gulve i bygninger er solide.

Alle yderdøre er udenfor åbningstid sikret med alarmer og låse, på nær receptionen indenfor almindelig arbejdstid, hvor indgangen er overvåget af receptionisten. Hvis receptionisten bliver nødt til at forlade receptionen – også blot kortvarigt - aflåses indgangen.

Døre og vinduer er låste, når de ikke er under opsyn.

Det er installeret branddøre og indbrudsalarmer

8.1.2. Fysisk adgangskontrol
Adgang til serverrummet eller andre områder, hvor fortrolig information behandles eller lagres er begrænset til autoriserede personer ved fysisk lås

8.1.3 Sikring af kontorer, lokaler og faciliteter
Der er ingen forhold, som kan afsløre placeringen af serverrummet for uvedkommende, fx står der ikke "Serverrum" på døren til serverrummet.

8.1.4 Beskyttelse mod eksterne og miljømæssige trusler
Servere med vitale data er placeret i IT-center Nord

8.1.5 Arbejde i sikre områder
Kun personale, som har behov for kendskab til serverrummet eller andre sikre områder, har det.

Diverse eksterne teknikere får ikke lov at arbejde i serverrummet uden opsyn.

8.2 Udstyr

8.2.1 Placering og beskyttelse af udstyr
Udstyr er placeret, så unødvendig adgang til arbejdsområder minimeres

Diverse skærme med følsomme data er placeret sådan, at risikoen nedsættes for at uautoriserede personer kan se skærmene

Udstyr er placeret på sådan en måde, at risikoen for potentielle fysiske og miljømæssige trusler, fx tyveri, sprængstoffer, røg, vand, støv, vibration, kemiske virkninger, strømforstyrrelser, kommunikationsforstyrrelser, elektromagnetisk stråling og hærværk, minimeres

Der må ikke spises, drikkes eller ryges/dampes i serverrummet.

Temperatur og fugtighed i serverrummet overvåges.

Der er etableres lynbeskyttelse for alle bygninger og lynafledere på alle indkommende elektricitets- og kommunikationslinjer.

8.2.2 Understøttende forsyninger
Understøttende forsyninger f.eks. strømforsyninger, telekommunikation, vandforsyning, gas, afløb, ventilation og klimaanlæg inspiceres og testes med jævne mellermrum

Netværkets redundans er sikret ved, at der benyttes flere forsyningsindgange

8.2.3 Sikring af kabler
Kabler til elektricitet og telekommunikation er beskyttet, og der findes ingen synlige kabler

8.2.4 Vedligeholdelse af udstyr
Der udføres eftersyn på udstyr efter leverandørens anbefalinger. Det er kun godkendte personer, som udfører reparationer og vedligeholdelse på udstyr.

8.2.5 Fjernelse af aktiver
Udstyr, informationer og software må ikke fjernes fra organisationen uden tilladelse fra IT-afdeling eller administration

8.2.6 Sikring af udstyr og aktiver uden for organisationens lokaler
Al anvendelse af informationslagrings- og behandlingsudstyr uden for organisationen skal godkendes af ledelsen. Herunder hjemme- og fjernarbejdspladser.

8.2.7 Sikker bortskaffelse eller genbrug af udstyr
Det tjekkes, at informationer på alle lagringsmedier er slettet eller overskrevet inden bortskaffelse eller genbrug

8.2.8 Brugerudstyr uden opsyn
Brugere skal afslutte sessioner, når de er færdige, eller aktivere passwordbeskyttet pauseskærm.

Brugere skal logge af applikationer eller netværkstjenester, når de ikke længere bruges.

Brugere skal sikre computere eller mobilt udstyr mod uautoriseret brug ved hjælp af en nøglelås eller adgangskode, når det ikke er i brug.

8.2.9 Politik for ryddeligt skrivebord og blank skærm
Brugere skal holde deres skriveborde og arbejdsstationer ryddet for papir og flytbare lagringsmedier, når arbejdsstationen forlades.

Papir og elektroniske lagringsmedier skal låses inde, når de ikke benyttes.

Computere og terminaler skal være logget af eller beskyttet med skærmlås.

Dokumenter, som indeholder følsom eller klassificeret information skal straks fjernes fra printere.

9. Driftssikkerhed

9.1. Driftsprocedurer og ansvarsområder

9.1.1. Driftsafviklingsprocedurer
Der er etableret formelle driftsprocedurer, som gøres tilgængelige for de brugere, som har behov for dem.

Der er procedurer for:

- opstart og nedlukning af PC'er

- backup
- vedligeholdelse af udstyr
- mediehåndtering
- serverrum
- mailhåndtering og -sikkerhed
- overvågning

9.1.2. Ændringsstyring
Ændringer til systemer skal godkendes af systemejer. De potentielle konsekvenser for informationssikkerheden vurderes ifm. godkendelsen.

9.2 Malwarebeskyttelse
Brugerne er oplyst om, at de ikke må installere uautoriseret software, før de har fået det godkendt af IT.

Der er implementeret kontroller, som forhindrer eller sporer brugen af uautoriseret software

Der er implementeret kontroller, som forhindrer eller sporer brugen af ondsindede eller suspekte websites

9.3 Backup
Der tages fra IT-Center Nord og skolens IT-afdeling løbende backup af organisationens informationsaktiver og disse testes regelmæssigt.

Der tages fuld backup dagligt af fælles og personlige drev i administrationsafdelingen, samt af data i diverse grupper på Office 365 – der tages **IKKE** back up af data gemt på personlig Onedrive-platform

Backupkopierne opbevares adskilt fra organisationens hovedkontor via cloud og fysisk placering i IT-center Nords lokaler

10. Kommunikationssikkerhed
10.1 Styring af netværkssikkerhed
Gæstenetværk er separeret fra organisationens interne netværk.

Adgangen mellem netværksdomæner er styret ved hjælp af en firewall gateway.

Trådløse netværk er adskilt fra organisationens interne netværk.

10.2 Informationsoverførsel
10.2.1 Politikker og procedurer for informationsoverførsel
Følsomme oplysninger skal overføres krypteret via E-boks

Det er ikke tilladt at efterlade telefonsvarerbeskeder med følsomme oplysninger.

Det er ikke tilladt at have fortrolige samtaler på offentlige steder eller over usikre kommunikationskanaler i åbne kontorer eller mødesteder.

10.2.2 Elektroniske meddelelser
Brugerne skal være meget opmærksomme på at elektroniske meddelelser adresseres korrekt.

Det skal godkendes af IT-afdeling, før diverse instant message eller fildelingsværktøjer benyttes til at overføre informationer.

11. Anskaffelse, udvikling og vedligeholdelse af systemer
11.1 Sikkerhedskrav til informationssystemer
Krav til informationssikkerhed er omfattet af kravene, som stilles til nye informationssystemer eller forbedringer af eksisterende informationssystemer.

12. Leverandørforhold
12.1 Informationssikkerhed i leverandørforhold
12.1.1 Informationssikkerhed for leverandørforhold
Der er fokus på informationssikkerhedskrav med leverandører

12.1.2 Håndtering af sikkerhed i leverandøraftaler
Der udarbejdes detaljerede leverandøraftaler, hvor det er muligt for at undgå misforståelser mellem organisationen og leverandøren.

12.2 Styring af leverandørydelser

12.2.1 Overvågning og gennemgang af leverandørydelser
Leverandørydelser bliver overvåget, gennemgået og auditeret

13. Styring af informationssikkerhedsbrud

13.1 Styring af informationssikkerhedsbrud og forbedringer

13.1.1 Ansvar og procedure
IT Procedurer af fastlagt, således at det er kompetente medarbejdere, som håndterer brud. Der er etableret et fast kontaktpunkt for opdagelse og rapportering af brud.

Der er udarbejdet rapporteringsskemaer ved informationssikkerhedshændelser til at understøtte rapportering.

13.1.2 Rapportering af informationssikkerhedshændelser
Alle brugere har ansvar for hurtigst muligt at rapportere informationssikkerhedshændelser til IT-afdelingen eller administrationen

Situationer, der skal rapporteres, er ved mistanke om:

Ineffektiv sikkerhedsstyring	Menneskelige fejl	Ukontrollerede systemændringer	Brud på fysisk sikring
Brud på informationers forventede integritet, fortrolighed eller tilgængelighed	Overtrædelse af politikker eller retningslinjer	Fejl i software eller hardware	Brud på adgangskontrollerne

13.1.3 Rapportering af informationssikkerhedssvagheder
Alle brugere har pligt til at rapportere observererede svagheder i informationssystemer og tjenester til IT-afdeling eller administration. Det er ikke tilladt for almindelige brugere at forsøge at be- eller afkræfte en eventuel svaghed, da dette kan opfattes som et forsøg på at lave et sikkerhedsbrud.

13.1.4 Håndtering af informationssikkerhedsbrud
Ved brud bliver der:

- indsamlet beviser hurtigst muligt efter hændelsen
- hvis relevant, udarbejdet en kriminalteknisk analyse af informationssikkerheden
- foretaget fejlafhjælpning efter behov
- foretaget logning af alle involverede beredskabsaktiviteter for senere analyse
- kommunikeret om bruddet til andre interne og eksterne parter, der har behov for denne viden
- foretaget håndtering af den eller de informationssikkerhedssvagheder, som har forårsaget eller været medvirkende til bruddet
- foretaget formel lukning og registrering af bruddet efter en vellykket håndtering

Efter brud bliver der foretaget en analyse af identificerede kilder til bruddet.

13.1.5 Erfaring fra informationssikkerhedsbrud
Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, bliver anvendt til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.

13.1.6 Indsamling af beviser
Ansvaret for følgende bevisindsamling er placeret hos IT-afdeling og/eller administration:

Identifikation, indsamling, anskaffelse og opbevaring af bevismateriale, som tager højde for: chain of custody, sikring af beviser, sikring af medarbejdere, roller og ansvarsområder for involverede medarbejdere, medarbejderes kompetencer, dokumentation og orientering

14. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

14.1. Informationssikkerhedskontinuitet

14.1.1. Planlægning af informationssikkerhedskontinuitet
Kravene til informationssikkerhed er de samme i kritiske situationer som under normale forhold.

14.1.2 Implementering af informationssikkerhedskontinuitet
Der er udpeget beredskabspersonale med ansvar, bemyndigelse og kompetencer til at håndtere et sikkerhedsbrud og opretholde informationssikkerhed. Beredskabspersonalet er angivet i beredskabsplanen. Beredskabsplanen beskriver i detaljer, hvordan organisationen vil håndtere en ødelæggende hændelse og opretholde informationssikkerheden.

Prioriteten af handlinger i beredskabsplanen er baseret på en konsekvensanalyse af IT-aktivers tilgængelighed, således at de mest forretningskritiske systemer reetableres først.

Beredskabsplanen er gjort tilgængelig for alt relevant personale.

14.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten
Beredskabsplanen testes med jævne mellemrum minimum en gang årligt og opdateres efter behov.

14.2 Redundans

14.2.1 Tilgængelighed af informationsbehandlingsfaciliteter
Der er etableret redundans for informationsbehandlingsaktiviteter for at kunne imødekomme tilgængelighedskrav.

15. Overensstemmelse

15.1. Overensstemmelse med lov- og kontraktkrav

15.1.1. Identifikation af gældende lovgivning og kontraktkrav
Organisationen er opmærksom på, at vi er underlagt diverse lovgivning og kontraktkrav