**Erklæring om oplæring for Datatekniker med speciale i cybersikkerhed**

Erklæringen om oplæring er et dialogværktøj mellem lærling, erhvervsskole og oplæringsvirksomhed. Den indeholder en liste over de oplæringsmål, lærlingen skal nå gennem oplæringen i virksomheden. Metalindustriens Uddannelsesudvalg har udformet erklæringen om oplæring i henhold til gældende lov og bekendtgørelser om erhvervsuddannelserne.

Erklæringen om oplæring fremsendes af erhvervsskolen og udfyldes af oplæringsvirksomheden i samarbejde med lærlingen. Erklæringen om oplæring opbevares af virksomheden, og der sendes en kopi til erhvervsskolen samt til lærlingen.

**Nedenstående udfyldes af erhvervsskolen før fremsendelse til virksomheden**

|  |
| --- |
| Erklæringen om oplæring vedrører oplæringsperiode: 1 □ 2 □ 3 □ *Der kan være flere oplæringsperioder afhængig af, hvor mange skoleperioder den enkelte skole har opdelt skoleundervisningen i. Der skal dog mindst være to oplæringsperioder.* |

|  |  |
| --- | --- |
| Lærlingens navn: | CPR nr.: |

|  |  |
| --- | --- |
| Virksomhedens navn: | CVR nr.: |
| Virksomhedens adresse: | Tlf. nr.:  |
| Postnr. og by: | E-mail: |

|  |
| --- |
| Erhvervsskolens navn: |
| Kontaktlærer: | E-mail: |
| Kontaktlærerens tlf. nr.: | Skolens tlf. nr.:  |
| Meddelelse fra skolen: |
| Dato: |

**Nedenstående udfyldes af virksomheden ved oplæringsperiodens afslutning**

*Denne erklæring om oplæring vedrører de oplæringsperioder, der er placeret imellem skoleperioderne.*

*Der skal udfyldes en særlig skole- og virksomhedserklæring efter den afsluttende oplæringsperiode.*

I skemaet herunder skal ét af de tre felter afkrydses for hvert af oplæringsmålene:

* **Oplæring er ikke startet** – hvis lærlingen ikke har arbejdet med arbejdsområdet/funktionen
* **Oplæring er i gang** – hvis lærlingen har arbejdet med arbejdsområdet/funktionen, men endnu ikke har nået oplæringsmålet fuldt ud
* **Oplæringsmålet er nået** – hvis lærlingen har nået det beskrevne oplæringsmål for uddannelsen

Samtlige oplæringsmål skal være opfyldt ved afslutningen af den sidste oplæringsperiode. Det er derfor vigtigt, at virksomheden i hver oplæringsperiode overvejer inden for hvilke oplæringsmål, der skal igangsættes en oplæring af lærlingen.

Skemaet udfyldes af den ansvarlige for oplæring i virksomheden i samarbejde med lærlingen.

| **Oplæringsmål, som lærlingen skal have opnået ved uddannelsens afslutning** | **Oplæring** **er ikke** **startet** | **Oplæring er i gang** | **Oplærings-målet** **er nået** |
| --- | --- | --- | --- |
| Lærlingen skal forstå sikkerhedsaspekter ved cloud-baserede tjenester og implementere delt ansvar mellem kunde og udbyder. |  |  |  |
| Lærlingen skal anvende, Proaktiv informations- og cybersikkerhed, med udgangspunkt i virksomhedens overordnede forretningsmål, igennem anvendelse af informationsteknologier (IT) og operationelle teknologier (OT) og under hensyn til virksomhedens størrelse og kompleksitet. |  |  |  |
| Lærlingen skal designe og implementere sikre netværksarkitekturer, herunder segmentering og beskyttelse mod trusler. |  |  |  |
| Lærlingen skal bidrage til sikre kodningspraksisser og forstå OWASP-principper for at identificere og rette sårbarheder i applikationer. |  |  |  |
| Lærlingen skal installere og administrere firewalls samt intrusion detection/prevention systems for at sikre netværksgrænser. |  |  |  |
| Lærlingen skal designe og implementere identitets- og adgangsstyringssystemer, herunder multifaktorgodkendelse. |  |  |  |
| Udføre overvågning og analyse af sikkerhedshændelser ved hjælp af Security Information and Event Management (SIEM) systems. |  |  |  |
| Udføre sårbarhedsvurderinger og penetrationstest for at identificere og mitigere potentielle sikkerhedstrusler. |  |  |  |
| Udføre anvendelse af krypteringsteknikker til at beskytte data i transit og i ro. |  |  |  |
| Lærlingen skal udvikle, anvende og gennemføre hændelseshåndteringsplaner for effektivt at reagere på sikkerhedsbrud. |  |  |  |
| Lærlingen skal forstå og implementere krav fra relevante sikkerhedsstandarder og regulativer som ISO 27001, NIS2, CyberSecurity Act. og GDPR. |  |  |  |
| Lærlingen skal installere og integrere Extended Detection and Response for forbedret trusseldetektions- og responsfunktionalitet. |  |  |  |
| Lærlingen skal udføre implementering af konfigurationer og praksisser for at minimere risikoen for serverkompromittering. |  |  |  |
| Lærlingen skal anvende Cyber Risk Governance tools til at styre og overvåge cybersikkerhedsrisici og overensstemmelse. |  |  |  |
| Lærlingen skal udvikle og håndhæve netværkssikkerhedspolitikker, der beskytter organisationens infrastruktur. |  |  |  |
| Lærlingen skal installere og vedligeholde operative systemer med regelmæssig patching og sårbarhedsstyring. |  |  |  |
| Lærlingen skal bidrage til udvikling af programmer for medarbejdernes uddannelse og bevidstgørelse om bedste praksis inden for sikkerhed. |  |  |  |
| Lærlingen skal udføre regelmæssig gennemgang og analyse af logfiler for at opdage usædvanlige aktiviteter. |  |  |  |
| Lærlingen skal udføre evaluering af og styring af sikkerhedsrisici forbundet med tredjepartsleverandører og -tjenester. |  |  |  |
| Lærlingen skal bidrage til en omfattende sikkerhedsarkitektur, der omfatter alle lag af IT-infrastrukturen, fra applikationer til netværk og databaser samt processer. |  |  |  |
| Installere og konfigurere endpoint-sikkerhedsløsninger for at beskytte individuelle enheder mod malware og andre trusler. |  |  |  |
| Udføre regelmæssig backup af kritiske systemer og data, samt planlægge og teste gendannelsesprocedurer for at sikre dataenes tilgængelighed efter et sikkerhedsbrud med Air-gab. |  |  |  |
| Lærlingen skal bidrage til og udføre risikovurderinger for at identificere, analysere og prioritere sikkerhedstrusler og sårbarheder i organisationens infrastruktur. |  |  |  |
| Lærlingen skal udvikle og implementere sikkerhedsretningslinjer og standarder, der er i overensstemmelse med best practices og regulatoriske krav. |  |  |  |
| Udføre trusselanalyser for at vurdere potentielle sikkerhedsrisici og udvikle strategier til at mitigere disse. |  |  |  |
| Lærlingen skal gennemføre regelmæssige sikkerhedstests af systemer og applikationer for at identificere og afhjælpe svagheder. |  |  |  |
| Lærlingen skal forstå principperne for digital forensics og kunne anvende disse i tilfælde af sikkerhedshændelser. |  |  |  |
| Lærlingen skal forstå og udføre konstant overvågning af netværkstrafik, Server, Applikationer og Services for at opdage uregelmæssigheder og potentielle sikkerhedstrusler. |  |  |  |
| Lærlingen skal bidrage til oprettelse af strukturerede rapporteringsprocedurer for håndtering af sikkerhedshændelser og sikre, at alle medarbejdere er bekendt med dem. |  |  |  |
| Udføre årlige evalueringer af organisationens sikkerhedsprogram for at identificere forbedringsmuligheder og sikre overholdelse af standarder. |  |  |  |
| Lærlingen skal bidrage og anvende samt implementere en effektiv asset management-struktur, der sikrer, at alle aktiver (hardware og software samt processer) registreres, overvåges og vedligeholdes med henblik på at minimere sikkerhedsrisici. Dette inkluderer klassificering af aktiver baseret på følsomhed og kritikalitet, samt sikring af, at alle aktiver har de nødvendige sikkerhedsforanstaltninger på plads. |  |  |  |
| Lærlingen skal bidrage til at designe og implementere sikkerhedsforanstaltninger for lagringssystemer, der sikrer data mod uautoriseret adgang, tab eller ødelæggelse. Dette inkluderer konfiguration af netværkslagringssystemer (NAS) og storage area networks (SAN) med tilstrækkelige sikkerhedsfunktioner. |  |  |  |
| Lærlingen skal implementere data og og generel lifecycle management af Hardware og Software, for at styre, hvornår data opbevares, hvordan de beskyttes, og hvornår de skal slettes. |  |  |  |
| Lærlingen skal forstå og implementere change management-processer for at sikre, at alle ændringer i IT-systemerne gennemføres sikkert og kontrolleret. Dette inkluderer at følge etablerede procedurer for godkendelse, dokumentation og test af ændringer for at minimere risikoen for driftsforstyrrelser og sikkerhedsbrud. |  |  |  |
| Lærlingen skal udføre regelmæssige opdateringer af applikationer og systemer for at sikre, at de er beskyttet mod kendte sårbarheder. Dette inkluderer planlægning og koordinering af opdateringer for at minimere digitale risici. |  |  |  |
| Lærlingen skal implementere whitelisting for at sikre, at kun godkendte applikationer og programmer kan køre på virksomhedens systemer, hvilket reducerer risikoen for malware og uønskede programmer. |  |  |  |
| Lærlingen skal bidrage til forståelse for kodesikkerhed og udvikle metoder til at evaluere og forbedre sikkerheden i kode, samt sikre, at koden overholder branchens bedste praksisser bla. for test. |  |  |  |
| Lærlingen skal installere og konfigurere e-mail filtreringsløsninger for at beskytte organisationen mod phishing, spam og malware, der kan komme via e-mail. |  |  |  |
| Lærlingen skal implementere DNS-filtrering for at forhindre adgang til skadelige websteder og sikre, at al DNS-trafik overvåges og kontrolleres for ondsindede anmodninger. |  |  |  |
| Lærlingen skal anvende modenhedsvurdering af organisationens cybersikkerhed for at vurdere effektiviteten af de eksisterende sikkerhedstiltag. Dette inkluderer at identificere forbedringsområder og anbefale skridt til at øge den. |  |  |  |

|  |
| --- |
| Ansvarlig for oplæring i virksomheden |
| Navn:  |
| E-mail: | Tlf. nr.: |
| Vurderer virksomheden, at lærlingen har særlige behov med hensyn til den efterfølgende skoleundervisning eller oplæring? Nej, der er ingen særlige behov (sæt kryds) □Ja, jeg vil gerne kontaktes (sæt kryds) □Begrundelse: |
| Dato:  |