CIS Controls v8

Komplet tjekliste — 153 safeguards

Alle 18 kontrolgrupper med Implementation Group-markering,
danske beskrivelser, status-felter og plads til ansvarlig og deadline.

IG1	56 safeguards — grundlæggende cyberhygiejne
IG2	74 yderligere safeguards — mellemstor virksomhed
IG3	23 yderligere safeguards — avanceret sikkerhed

Udgivet af **GapGuard** — et produkt fra ITNU ApS
April 2026 · gapguard.dk

1. Inventar og kontrol af virksomhedsaktiver

Inventory and Control of Enterprise Assets

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
1.1	**Etablér og vedligehold et detaljeret inventar over virksomhedsaktiver** Opret og vedligehold en komplet liste over alle fysiske og virtuelle aktiver (servere, laptops, mobiler, IoT). Listen...	●	●	●	■		
1.2	**Håndtér uautoriserede aktiver** Hav en proces til at identificere og håndtere uautoriserede enheder på netværket. Bloker eller isolér enheder der ikk...	●	●	●	■		
1.3	**Anvend et aktivt opdagelsesværktøj** Brug et aktivt scanningsværktøj (f.eks. Nmap, Lansweeper, SCCM) til at opdage nye enheder på netværket. Kør scanninge...		●	●	■		
1.4	**Brug DHCP-logning til at opdatere aktivinventar** Aktivér DHCP-logning og brug data til automatisk at opdatere aktivinventaret. Giver overblik over enheder der dynamis...		●	●	■		
1.5	**Anvend et passivt opdagelsesværktøj** Supplér aktiv scanning med passiv overvågning (f.eks. netflow, TAP) til at opdage enheder der ikke svarer på aktive p...			●	■		

2. Inventar og kontrol af softwareaktiver

Inventory and Control of Software Assets

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
2.1	**Etablér og vedligehold et softwareinventar** Opret en komplet liste over al autoriseret software med version, leverandør og forretningsformål. Opdatér ved ændring...	●	●	●	■		
2.2	**Sikr at autoriseret software er understøttet** Sikr at al software i brug er aktivt understøttet af leverandøren med sikkerhedsopdateringer. Udarbejd plan for udfas...	●	●	●	■		
2.3	**Håndtér uautoriseret software** Fjern eller bloker uautoriseret software inden for 24-48 timer efter opdagelse. Brug GPO, MDM eller endpoint manageme...	●	●	●	■		
2.4	**Anvend automatiserede softwareinventarværktøjer** Implementér automatiserede værktøjer (SCCM, Intune, osquery) til løbende opdagelse og inventarisering af installeret ...		●	●	■		
2.5	**Godkendelsesliste for autoriseret software** Implementér application whitelisting så kun godkendt software kan eksekvere. Start med servere og kritiske systemer, ...		●	●	■		
2.6	**Godkendelsesliste for autoriserede biblioteker** Begræns hvilke softwarebiblioteker (DLL, .so, npm, pip) der må bruges i udviklings- og produktionsmiljøer.		●	●	■		
2.7	**Godkendelsesliste for autoriserede scripts** Tillad kun godkendte scripts at køre. Brug PowerShell Constrained Language Mode, AppLocker eller lignende til at blok...			●	■		

3. Databeskyttelse

Data Protection

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
3.1	**Etablér og vedligehold en datastyringsproces** Etablér en formel datastyringsproces der definerer roller, ansvar og procedurer for datahåndtering gennem hele livscy...	●	●	●	■		
3.2	**Etablér og vedligehold et datainventar** Opret et datainventar der identificerer alle følsomme data, deres placering, ejer og klassifikation. Inkludér både st...	●	●	●	■		
3.3	**Konfigurér adgangskontrollister for data** Konfigurér adgangskontrollister (ACL) baseret på principle of least privilege. Gennemgå adgangsrettigheder minimum kv...	●	●	●	■		
3.4	**Håndhæv dataopbevaring** Definér og håndhæv opbevaringsperioder for alle datatyper. Slet data systematisk når opbevaringsperioden udløber.	●	●	●	■		
3.5	**Sikker bortskaffelse af data** Sikr forsvarlig destruktion af data på alle medier (diske, USB, papir). Brug certificeret sletning eller fysisk destr...	●	●	●	■		
3.6	**Kryptér data på slutbrugerenheder** Aktivér fuld diskkryptering (BitLocker, FileVault) på alle bærbare enheder. Centraliser nøglehåndtering.	●	●	●	■		
3.7	**Etablér og vedligehold en dataklassifikation** Etablér et klassifikationsskema (f.eks. Offentlig, Intern, Fortrolig, Strengt fortrolig) og mærk alle data derefter.		●	●	■		
3.8	**Dokumentér dataflows** Dokumentér hvordan følsomme data bevæger sig gennem organisationen — fra oprettelse til sletning, inklusiv tredjeparter.		●	●	■		
3.9	**Kryptér data på flytbare medier** Kryptér alle flytbare medier (USB, eksterne diske) der indeholder følsomme data. Overvej at blokere USB helt.		●	●	■		
3.10	**Kryptér følsomme data under overførsel** Sikr at al følsom data krypteres under overførsel via TLS 1.2+, VPN eller tilsvarende. Gælder intern og ekstern kommu...		●	●	■		
3.11	**Kryptér følsomme data i hvile** Kryptér følsomme data i hvile (databaser, filshares, backups). Brug AES-256 og centraliser nøglehåndtering.		●	●	■		
3.12	**Segmentér databehandling og lagring efter følsomhed** Adskil lagring og behandling af data baseret på klassifikation. Følsomme data bør ikke ligge sammen med offentlige data.		●	●	■		
3.13	**Implementér en Data Loss Prevention-løsning** Implementér DLP-løsning der overvåger og blokerer uautoriseret overførsel af følsomme data via e-mail, cloud, USB mv.			●	■		
3.14	**Logning af adgang til følsomme data** Log al adgang til følsomme data med hvem, hvad, hvornår. Overvåg for usædvanlige adgangsmønstre.			●	■		

4. Sikker konfiguration af aktiver og software

Secure Configuration of Enterprise Assets and Software

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
4.1	**Etablér og vedligehold en sikker konfigurationsproces** Etablér og vedligehold sikre baseline-konfigurationer for alle aktivtyper. Brug CIS Benchmarks eller leverandørens ha...	●	●	●	■		
4.2	**Etablér sikker konfiguration for netværksinfrastruktur** Hærd netværksudstyr (firewalls, switches, routere, AP'er) med sikre konfigurationer. Deaktivér unødvendige services o...	●	●	●	■		
4.3	**Konfigurér automatisk sessionslåsning** Konfigurér automatisk skærmlås efter max 15 minutters inaktivitet på alle enheder.	●	●	●	■		
4.4	**Implementér og administrér firewall på servere** Implementér host-baseret firewall på alle servere. Tillad kun nødvendig indgående og udgående trafik.	●	●	●	■		
4.5	**Implementér og administrér firewall på slutbrugerenheder** Aktivér og konfigurér den indbyggede firewall på alle slutbrugerenheder. Centraliser policy via GPO eller MDM.	●	●	●	■		
4.6	**Sikker administration af aktiver og software** Administrér alle aktiver via sikre protokoller (SSH, HTTPS). Undgå klartekst-protokoller som Telnet og HTTP til admin...	●	●	●	■		
4.7	**Administrér standardkonti på virksomhedsaktiver** Skift eller deaktivér alle standardkonti og -adgangskoder på netværksudstyr, servere og applikationer før idriftsætte...	●	●	●	■		
4.8	**Afinstallér eller deaktivér unødvendige tjenester** Identificér og deaktivér alle unødvendige tjenester, porte og protokoller. Dokumentér forretningsbehovet for tilbagev...		●	●	■		
4.9	**Konfigurér pålidelige DNS-servere** Konfigurér alle enheder til at bruge organisationens godkendte DNS-servere. Overvej DNS-filtrering til sikkerhed.		●	●	■		
4.10	**Håndhæv automatisk enhedslåsning på bærbare enheder** Aktivér automatisk enhedslås efter max 5 mislykkede loginforsøg på mobile enheder.		●	●	■		
4.11	**Håndhæv fjernsletningsmulighed på bærbare enheder** Sikr at alle mobile enheder kan fjernslettes ved tab eller tyveri. Test proceduren regelmæssigt.		●	●	■		
4.12	**Adskil virksomhedsarbejdsområder på mobile enheder** Brug containerisering eller work profile til at adskille virksomhedsdata fra personlige data på BYOD-enheder.			●	■		

5. Kontoadministration

Account Management

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
5.1	**Etablér og vedligehold et kontoinventar** Opret et komplet inventar over alle brugerkonti (inkl. service-, admin- og gæstekonti) med ejer og sidst aktive dato.	●	●	●	■		

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
5.2	**Brug unikke adgangskoder** Kræv unikke, komplekse adgangskoder (min. 14 tegn) for alle konti. Implementér password manager til organisationen.	●	●	●	■		
5.3	**Deaktivér inaktive konti** Deaktivér konti der ikke har været aktive i 45 dage. Gennemgå kontolisten minimum månedligt.	●	●	●	■		
5.4	**Begræns administratorrettigheder til dedikerede konti** Brug dedikerede administratorkonti der er adskilt fra daglige brugerkonti. Admin-konti må ikke bruges til e-mail elle...	●	●	●	■		
5.5	**Etablér og vedligehold et inventar over servicekonti** Opret et inventar over alle servicekonti med ejer, formål og sidst reviewet dato. Roter passwords regelmæssigt.		●	●	■		
5.6	**Centralisér kontoadministration** Centralisér kontoadministration via Active Directory, Azure AD eller lignende. Undgå lokale konti på individuelle sys...		●	●	■		

6. Adgangskontrol

Access Control Management

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
6.1	**Etablér en proces for tildeling af adgang** Etablér en formel proces for tildeling af adgang med godkendelse fra dataejer. Dokumentér alle adgangsanmodninger.	●	●	●	■		
6.2	**Etablér en proces for fjernelse af adgang** Hav en proces for øjeblikkelig fjernelse af adgang ved fratræden og periodisk review ved rolleændring.	●	●	●	■		
6.3	**Kræv MFA for eksternt eksponerede applikationer** Kræv MFA for alle eksternt tilgængelige applikationer (webmail, VPN, cloud-tjenester, RDP).	●	●	●	■		
6.4	**Kræv MFA for fjernnetværksadgang** Kræv MFA for al fjernadgang til organisationens netværk via VPN eller lignende.	●	●	●	■		
6.5	**Kræv MFA for administrativ adgang** Kræv MFA for alle administrative handlinger og privilegerede konti — uden undtagelser.	●	●	●	■		
6.6	**Etablér et inventar over autentificeringssystemer** Opret et inventar over alle autentificeringssystemer (AD, LDAP, SAML, OAuth) med version og konfiguration.		●	●	■		
6.7	**Centralisér adgangskontrol** Centralisér adgangskontrol via SSO og rollebaseret adgangsstyring. Reducer antallet af separate loginsystemer.		●	●	■		
6.8	**Definér og vedligehold rollebaseret adgangskontrol** Definér og implementér RBAC (Role-Based Access Control) med klare roller og tilhørende rettigheder. Review minimum ha...			●	■		

7. Kontinuerlig sårbarhedshåndtering

Continuous Vulnerability Management

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
7.1	**Etablér og vedligehold en sårbarhedshåndteringsproces** Etablér en formel sårbarhedshåndteringsproces med roller, ansvar, scanningsfrekvens og SLA'er for patching.	●	●	●	■		
7.2	**Etablér og vedligehold en udbedringssproces** Definér SLA'er for udbedring baseret på alvorlighed: Kritisk (48t), Høj (7d), Medium (30d), Lav (90d).	●	●	●	■		
7.3	**Udfør automatisk OS-patchhåndtering** Implementér automatisk OS-patching via WSUS, SCCM, Intune eller lignende. Patch kritiske systemer inden for 48 timer.	●	●	●	■		
7.4	**Udfør automatisk applikationspatchhåndtering** Automatisér patching af tredjepartsapplikationer (browsere, Java, Adobe). Brug værktøjer som Ninite, PDQ eller Intune.	●	●	●	■		
7.5	**Udfør automatiske sårbarhedsscanninger af interne aktiver** Kør automatiserede sårbarhedsscanninger af interne aktiver minimum månedligt. Prioritér kritiske fund til øjeblikkeli...		●	●	■		
7.6	**Udfør automatiske sårbarhedsscanninger af eksterne aktiver** Scan eksternt eksponerede aktiver (websites, mail, VPN) minimum månedligt. Overvej kontinuerlig scanning.		●	●	■		
7.7	**Udbedring af opdagede sårbarheder** Følg op på alle fundne sårbarheder med dokumenteret udbedring eller risikoaccept. Track status i et centralt system.		●	●	■		

8. Logadministration

Audit Log Management

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
8.1	**Etablér og vedligehold en logadministrationsproces** Etablér en logpolitik der definerer hvad der logges, hvor længe logs opbevares, og hvem der har adgang til dem.	●	●	●	■		
8.2	**Indsaml auditlogs** Aktivér auditlogning på alle kritiske systemer: OS, applikationer, databaser, netværksudstyr og sikkerhedsløsninger.	●	●	●	■		
8.3	**Sikr tilstrækkelig loglagring** Sikr tilstrækkelig lagerplads til logdata. Overvåg logvolumen og sæt alarmer ved kapacitetsproblemer.	●	●	●	■		
8.4	**Standardisér tidssynkronisering** Synkronisér alle systemer mod en fælles NTP-kilde for at sikre konsistente tidsstempler på tværs af logs.		●	●	■		
8.5	**Indsaml detaljerede auditlogs** Log detaljerede hændelser inkl. bruger-ID, kilde-IP, destination, handling og resultat.		●	●	■		
8.6	**Indsaml DNS-forespørgselslogge** Log alle DNS-forespørgsler for at opdage malware-kommunikation, data-exfiltration og policy-overtrædelser.		●	●	■		
8.7	**Indsaml URL-forespørgselslogge** Log alle URL-forespørgsler fra proxyer og firewalls. Brug til trusselsefterforskning og policy-håndhævelse.		●	●	■		

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
8.8	**Indsaml kommandolinjelogge** Log alle kommandolinjeaktiviteter (PowerShell, Bash, CMD) på servere og kritiske workstations.		●	●	■		
8.9	**Centralisér auditlogs** Send alle logs til et centralt SIEM-system for korrelation og analyse. Sikr logs mod manipulation.		●	●	■		
8.10	**Opbevar auditlogs** Opbevar logs minimum 90 dage online og 1 år arkiveret. Tilpas efter regulatoriske krav.		●	●	■		
8.11	**Udfør gennemgang af auditlogs** Gennemgå logs regelmæssigt for mistænkelig aktivitet. Opsæt automatiserede alarmer for kritiske hændelser.		●	●	■		
8.12	**Indsaml leverandørlogge** Indsaml og gennemgå sikkerhedslogs fra cloud- og SaaS-leverandører. Integrér med centralt SIEM.			●	■		

9. E-mail- og webbrowserbeskyttelse

Email and Web Browser Protections

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
9.1	**Sikr brug af kun fuldt understøttede browsere og e-mailklienter** Tillad kun understøttede versioner af browsere og e-mailklienter. Bloker eller opgradér forældede versioner automatisk.	●	●	●	■		
9.2	**Brug DNS-filtreringstjenester** Implementér DNS-filtrering (f.eks. Cisco Umbrella, Cloudflare Gateway) til at blokere kendte ondsindede domæner.	●	●	●	■		
9.3	**Vedligehold og håndhæv netværksbaserede URL-filtre** Implementér URL-filtrering på netværksniveau der blokerer adgang til kendte ondsindede og policy-stridende websites.		●	●	■		
9.4	**Begræns unødvendige browser- og e-mailudvidelser** Begræns browserudvidelser til en godkendt liste. Bloker installation af uautoriserede udvidelser via GPO eller MDM.		●	●	■		
9.5	**Implementér DMARC** Implementér DMARC, SPF og DKIM for alle e-maildomæner. Start med p=none, opgrader til p=reject.		●	●	■		
9.6	**Blokér unødvendige filtyper** Bloker modtagelse af potentielt farlige filtyper via e-mail (.exe, .scr, .js, .vbs, .ps1, makroaktiverede filer).		●	●	■		
9.7	**Implementér anti-malware på e-mailservere** Implementér anti-malware scanning på e-mailservere med sandboxing af vedhæftede filer og URL-rewriting.		●	●	■		

10. Malwareforsvar

Malware Defenses

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
10.1	**Implementér og vedligehold anti-malware software** Installér og vedligehold anti-malware/EDR på alle endpoints og servere. Sikr central management og rapportering.	●	●	●	■		
10.2	**Konfigurér automatiske anti-malware signatur-opdateringer** Konfigurér automatisk opdatering af malware-signaturer minimum dagligt. Overvåg at opdateringer gennemføres.	●	●	●	■		
10.3	**Deaktivér autorun og autoplay for flytbare medier** Deaktivér autorun og autoplay for USB og andre flytbare medier via GPO på alle Windows-systemer.	●	●	●	■		
10.4	**Konfigurér automatisk anti-malware scanning af flytbare medier** Konfigurér automatisk scanning af flytbare medier ved tilslutning. Overvej at blokere USB-enheder helt.		●	●	■		
10.5	**Aktivér anti-udnyttelsesfunktioner** Aktivér exploit protection / ASLR / DEP på alle endpoints. I Windows: aktiver via Windows Security.		●	●	■		
10.6	**Centralisér administration af anti-malware software** Administrér anti-malware centralt via en management-konsol. Overvåg status, opdateringer og detektioner.		●	●	■		
10.7	**Brug adfærdsbaseret anti-malware software** Implementér adfærdsbaseret malware-detektion (EDR/XDR) der kan opdage zero-day trusler og fileless attacks.		●	●	■		

11. Datagendannelse

Data Recovery

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
11.1	**Etablér og vedligehold en datagendannelsesproces** Etablér en formel backup-politik der definerer hvad der sikkerhedskopieres, hvor ofte, opbevaringstid og testfrekvens.	●	●	●	■		
11.2	**Udfør automatiserede sikkerhedskopier** Automatisér sikkerhedskopiering af alle kritiske data og systemer. Verificér dagligt at backup-jobs gennemføres.	●	●	●	■		
11.3	**Beskyt gendannelsesdata** Beskyt backupdata mod uautoriseret adgang og ransomware. Brug kryptering og adskil backup-credentials fra produktion.	●	●	●	■		
11.4	**Etablér en isoleret instans af gendannelsesdata** Opbevar mindst én backupkopi offline eller i et isoleret miljø (air-gapped) der ikke kan nås fra produktionsnetværket.	●	●	●	■		
11.5	**Test datagendannelse** Test gendannelse fra backup minimum kvartalsvis. Dokumentér gendannelsestider og verificér dataintegritet.		●	●	■		

12. Netværksinfrastruktur

Network Infrastructure Management

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
12.1	**Sikr at netværksinfrastruktur er opdateret** Hold al netværksudstyr opdateret med seneste firmware og sikkerhedspatches. Udskift udstyr der ikke længere understøt...	●	●	●	■		
12.2	**Etablér en sikker netværksarkitektur** Design netværket med segmentering (VLAN, firewall-zoner) baseret på dataklassifikation og risiko.		●	●	■		
12.3	**Sikker administration af netværksinfrastruktur** Administrér netværksudstyr via dedikerede management-VLAN med stærk autentificering og kryptering.		●	●	■		
12.4	**Etablér og vedligehold arkitekturdiagrammer** Opret og vedligehold aktuelle netværksdiagrammer inkl. alle segmenter, firewalls, forbindelser og dataflows.		●	●	■		
12.5	**Centralisér netværks-AAA** Centralisér netværksautentificering via RADIUS/TACACS+ for al administration af netværksudstyr.		●	●	■		
12.6	**Brug sikre netværksadministrationsprotokoller** Brug kun sikre protokoller til netværksadministration (SSH, HTTPS, SNMPv3). Deaktivér Telnet, HTTP og SNMPv1/v2.		●	●	■		
12.7	**Sikr at fjernenheder bruger VPN og virksomheds-AAA** Kræv VPN med MFA for alle fjernarbejdende medarbejdere. Sikr at split tunneling er deaktiveret eller kontrolleret.		●	●	■		
12.8	**Dedikerede computerressourcer til administrativt arbejde** Brug dedikerede administrative workstations (PAW/SAW) til administration af kritisk infrastruktur.			●	■		

13. Netværksovervågning og forsvar

Network Monitoring and Defense

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
13.1	**Centralisér sikkerhedshændelsesalarmering** Opsæt centraliseret alarmering for sikkerhedshændelser fra alle kritiske systemer. Definér eskaleringsprocesser.		●	●	■		
13.2	**Implementér en værtsbaseret indtrængningsdetektering** Implementér HIDS/EDR på kritiske servere og endpoints til detektion af uautoriserede ændringer og indtrængen.		●	●	■		
13.3	**Implementér en netværksbaseret indtrængningsdetektering** Implementér netværksbaseret IDS/IPS (f.eks. Suricata, Snort) på kritiske netværkssegmenter.		●	●	■		
13.4	**Udfør trafikfiltrering mellem netværkssegmenter** Implementér firewall-regler mellem alle netværkssegmenter. Tillad kun nødvendig, dokumenteret trafik.		●	●	■		
13.5	**Administrér adgangskontrol for fjernaktiver** Håndhæv adgangskontrol for fjernenheder via NAC, compliance-check eller Zero Trust-principper.		●	●	■		

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
13.6	**Indsaml netværkstrafiklogge** Indsaml netflow-data fra routere og switches. Brug til anomali-detektion og forensics.		●	●	■		
13.7	**Implementér en værtsbaseret indtrængningsforebyggelse** Implementér værtsbaseret IPS der aktivt blokerer kendte angrebsmønstre på kritiske systemer.			●	■		
13.8	**Implementér en netværksbaseret indtrængningsforebyggelse** Implementér netværksbaseret IPS inline der blokerer ondsindet trafik i realtid.			●	■		
13.9	**Implementér portniveau-adgangskontrol** Implementér adgangskontrol på alle remote management-porte (RDP, SSH). Brug jump-servere.			●	■		
13.10	**Anvend og fasthold sessionslås** Implementér application-layer filtering der kan inspicere og filtrere trafik baseret på applikationsindhold.			●	■		
13.11	**Justér tærskler for sikkerhedshændelsesalarmering** Justér løbende alarmeringstærskler baseret på falske positive og ændringer i trusselslandskabet.			●	■		

14. Sikkerhedsbevidsthed og træning

Security Awareness and Skills Training

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
14.1	**Etablér og vedligehold et sikkerhedsbevidsthedsprogram** Etablér et formelt awareness-program med regelmæssig træning for alle medarbejdere. Minimum årligt med løbende påmind...	●	●	●	■		
14.2	**Træn medarbejdere i at genkende social engineering-angreb** Træn alle medarbejdere i at genkende phishing, vishing, smishing og social engineering. Kør simulerede phishing-tests.	●	●	●	■		
14.3	**Træn medarbejdere i bedste praksis for autentificering** Undervis i adgangskodehygiejne: unikke passwords, password managers, og aldrig dele credentials.	●	●	●	■		
14.4	**Træn medarbejdere i bedste praksis for datahåndtering** Træn medarbejdere i korrekt datahåndtering baseret på klassifikation. Inkludér sikker deling og opbevaring.	●	●	●	■		
14.5	**Træn medarbejdere i årsager til utilsigtet dataeksponering** Undervis i årsager til utilsigtet dataeksponering: forkert adresserede mails, offentlige fildelinger, printudskrifter.	●	●	●	■		
14.6	**Træn medarbejdere i at genkende og rapportere sikkerhedshændelser** Træn alle i at genkende og rapportere sikkerhedshændelser. Gør rapporteringsprocessen nem og straffri.	●	●	●	■		
14.7	**Træn medarbejdere i at identificere manglende sikkerhedsopdateringer** Lær medarbejdere at genkende manglende opdateringer og rapportere systemer der ikke er patchet.	●	●	●	■		
14.8	**Træn medarbejdere i farerne ved usikre netværk** Undervis i risici ved offentlige WiFi-netværk, deling af skærm i det offentlige, og usikrede netværksforbindelser.	●	●	●	■		

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
14.9	**Udfør rollespecifik sikkerhedsbevidsthedstræning** Giv rollespecifik sikkerhedstræning til IT-medarbejdere, udviklere, ledelse og andre nøgleroller.		●	●	■		

15. Leverandørstyring

Service Provider Management

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
15.1	**Etablér og vedligehold et leverandørinventar** Opret et komplet inventar over alle IT-leverandører og serviceudbydere med kontaktinfo, kontrakt og dataadgang.	●	●	●	■		
15.2	**Etablér en leverandørstyringspolitik** Etablér en leverandørstyringspolitik der definerer krav til sikkerhed, databeskyttelse og incident-håndtering.		●	●	■		
15.3	**Klassificér leverandører** Klassificér leverandører efter risiko baseret på deres adgang til data og systemer. Prioritér tilsyn derefter.		●	●	■		
15.4	**Sikr at kontrakter indeholder sikkerhedskrav** Sikr at alle leverandørkontrakter indeholder sikkerhedskrav, SLA'er, ret til audit og krav om notifikation ved brud.		●	●	■		
15.5	**Vurdér leverandører** Vurdér leverandørers sikkerhedsniveau regelmæssigt via spørgeskemaer, certificeringer (ISO 27001) eller uafhængige au...			●	■		
15.6	**Overvåg leverandører** Overvåg løbende leverandørers sikkerhedsstatus. Brug tjenester som SecurityScorecard eller BitSight.			●	■		
15.7	**Sikker afvikling af leverandører** Hav en proces for sikker afvikling af leverandørforhold inkl. tilbagelevering af data, sletning og revokering af adgang.			●	■		

16. Applikationssikkerhed

Application Software Security

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
16.1	**Etablér en sikker applikationsudviklingsproces** Etablér en sikker udviklingsproces (SDLC) med sikkerhedskrav i alle faser fra design til deployment.		●	●	■		
16.2	**Proces for håndtering af softwaresårbarheder** Hav en proces til at modtage og håndtere rapporterede sårbarheder i egne applikationer.		●	●	■		
16.3	**Udfør rodårsagsanalyse af sikkerhedssårbarheder** Udfør root cause analyse på sikkerhedssårbarheder for at forebygge gentagelser.		●	●	■		
16.4	**Inventar over tredjepartskomponenter** Opret inventar over alle tredjepartskomponenter (open source, biblioteker, frameworks) med version og kendte sårbarhe...		●	●	■		

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
16.5	**Brug opdaterede og pålidelige tredjepartskomponenter** Hold alle tredjepartskomponenter opdaterede. Abonnér på sikkerhedsadvisories for anvendte komponenter.		●	●	■		
16.6	**Alvorlighedsvurderingssystem for applikationssårbarheder** Implementér et system til at vurdere alvorligheden af applikationssårbarheder (f.eks. CVSS).		●	●	■		
16.7	**Standard hærdningskonfigurationsskabeloner** Opret standardiserede hærdningsskabeloner for applikationsplatforme (webservere, databaser, app-servere).		●	●	■		
16.8	**Adskil produktions- og ikke-produktionssystemer** Adskil produktions-, test- og udviklingsmiljøer fysisk eller logisk. Brug aldrig produktionsdata i test.		●	●	■		
16.9	**Træn udviklere i applikationssikkerhed** Træn udviklere i sikker kodning (OWASP Top 10, input-validering, output-encoding, sikker session-håndtering).		●	●	■		
16.10	**Anvend sikre designprincipper i arkitekturer** Anvend sikre designprincipper: defense in depth, least privilege, secure defaults, fail secure.		●	●	■		
16.11	**Brug godkendte moduler til sikkerhedskomponenter** Brug gennemtestede og vedligeholdte sikkerhedsmoduler til kryptografi, autentificering og inputvalidering.		●	●	■		
16.12	**Implementér sikkerhedstjek på kodeniveau** Implementér statisk og dynamisk kodeanalyse (SAST/DAST) i CI/CD-pipelinen.			●	■		
16.13	**Udfør applikationspenetrationstest** Udfør penetrationstest af forretningskritiske applikationer minimum årligt og efter større ændringer.			●	■		
16.14	**Udfør trusselsmodellering** Udfør trusselsmodellering (f.eks. STRIDE) for nye applikationer og ved større arkitekturændringer.			●	■		

17. Hændelseshåndtering

Incident Response Management

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
17.1	**Udpeg personale til hændelseshåndtering** Udpeg en incident response-ansvarlig med klart defineret ansvar og myndighed til at eskalere.	●	●	●	■		
17.2	**Kontaktoplysninger til rapportering af sikkerhedshændelser** Vedligehold opdaterede kontaktlister for intern og ekstern rapportering af sikkerhedshændelser (inkl. myndigheder).	●	●	●	■		
17.3	**Virksomhedsproces for rapportering af hændelser** Etablér en enkel, tilgængelig proces som alle medarbejdere kan bruge til at rapportere mistænkelige hændelser.	●	●	●	■		
17.4	**Etablér en hændelsesresponsproces** Dokumentér en incident response-plan med faser: forberedelse, identifikation, inddæmning, udryddelse, gendannelse, op...		●	●	■		

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
17.5	**Tildel nøgleroller og ansvarsområder** Tildel nøgleroller i incident response-teamet: incident manager, teknisk lead, kommunikation, juridisk.		●	●	■		
17.6	**Kommunikationsmekanismer under hændelsesrespons** Etablér sikre, alternative kommunikationskanaler til brug under hændelser (mobil, Signal, out-of-band).		●	●	■		
17.7	**Udfør rutinemæssige hændelsesresponsøvelser** Gennemfør tabletop-øvelser eller simulerede hændelser minimum halvårligt for at teste incident response-planen.		●	●	■		
17.8	**Udfør evaluering efter hændelser** Udfør post-incident review efter alle væsentlige hændelser. Dokumentér learnings og opdater procedurer.		●	●	■		
17.9	**Etablér tærskler for sikkerhedshændelser** Definér tærskler for hvornår en hændelse eskaleres fra observation til incident til krise.		●	●	■		

18. Penetrationstest

Penetration Testing

ID	Safeguard	IG1	IG2	IG3	Status	Ansvarlig	Deadline
18.1	**Etablér et penetrationstestprogram** Etablér et penetrationstestprogram med defineret scope, frekvens og kvalifikationskrav til testere.		●	●	■		
18.2	**Udfør periodiske eksterne penetrationstest** Udfør ekstern penetrationstest minimum årligt, udført af kvalificerede, uafhængige testere.		●	●	■		
18.3	**Udbedring af penetrationstestfund** Udbedring af penetrationstestfund inden for definerede SLA'er. Track status til alle er lukket eller accepteret.		●	●	■		
18.4	**Validér sikkerhedsforanstaltninger** Validér at implementerede sikkerhedsforanstaltninger faktisk virker som forventet via teknisk verifikation.			●	■		
18.5	**Udfør periodiske interne penetrationstest** Udfør intern penetrationstest minimum årligt for at identificere laterale bevægelsesmuligheder og privilegieeskalering.			●	■		

Træt af at udfylde tjeklisten manuelt?

GapGuard automatiserer din GAP-analyse med dashboards,
multi-framework mapping (CIS ↔ NIS2 ↔ ISO 27001),
PDF-rapporter og årshjul — på dansk og engelsk.

→ Prøv GapGuard gratis i 7 dage

→ Book en demo

GapGuard — et produkt fra ITNU ApS · CVR 45557510
gapguard.dk · info@gapguard.dk