SIKKERHEDSFORANSTALTNINGER

Gældende fra d. 16. august 2022

Indledning

I det følgende beskrives .legals tekniske og organisatoriske sikkerhedsforanstaltninger for Tjenesterne. Derudover udarbejdes årligt en revisionserklæring, ISAE-3402 eller tilsvarende, som kan downloades her.

Risikostyring

Årlig risikovurdering

Direktionen i .legal A/S laver minimum én gang årligt en risikovurdering, der omfatter IT-installationerne og brugen heraf. Der tages udgangspunkt i det nuværende trusselbillede samt ny viden på området, der tilsammen danner grundlag for nye sikkerhedsinitiativer.

Retningslinjer og kontrolmål

Vi har internt dokumenteret en række kontrolmål, der anvendes til at kontrollere og sikre at vores sikkerhedspolitikker overholdes.

Kontrolmålene indeholder:

A. Formål: Beskriver hvorfor kontrolmålet er etableret og sikrer, at det afspejler den overordnede retningslinje for ISO-afsnittet.

B. Målepunkt: Beskriver hvordan kontrolmålet skal vurderes, således at der etableres et tilfredsstillende datagrundlag, og så målingen kan gennemføres inden for det tidsinterval, der er beskrevet, hvilket sikrer, at målet er specifikt og målbart.

C. Tærskel: Viser, hvad der kræves for at kontrolmålet overholdes.

Til opfølgning og dokumentation på de interne kontrolmål benyttes PACTIUS.

Informationssikkerhedspolitikker

IT Sikkerhedspolitik

.legal arbejder efter en IT sikkerhedspolitik som dækker Tjenesterne. IT sikkerhedspolitikken er organiseret efter ISO 27001:2013 og danner grundlag for de involveredes omgang med Tjenesterne. IT sikkerhedspolitikken er organiseret efter de standardiserede ISO-områder.

Opfølgningen på om kravene overholdes sker i henhold til en række retningslinjer og kontrolmål, der er beskrevet i politikken for hvert ISO-område.

IT sikkerhedspolitikken er godkendt af ledelsen og offentliggjort i virksomheden, herunder kommunikeret til relevante ansatte og samarbejdspartnere. for at sikre at IT sikkerhedspolitikken er passende, tilstrækkelig og effektiv, revurderes IT sikkerhedspolitikken minimum én gang årligt eller ved omfattende ændringer i organisationen, som har indflydelse på informationssikkerheden.

Organisation af informationssikkerhed

IT Sikkerhedsansvarlig

.legal har en overordnet IT sikkerhedsansvarlig med ansvar for den organisatoriske samt systemmæssige sikkerhed.

Funktionsadskillelse

.legal arbejder med funktionsadskillelse, for at sikre, at medarbejdere alene får adgang til informationer, der er påkrævet for at udføre deres funktion. Der arbejdes med funktionerne "administration", "salg", "udvikling", "support" og "drift".

Vi revurderer regelmæssigt alle medarbejderes adgange for at sikre, at adgangene fortsat stemmer overens med deres jobfunktion.

Personalesikkerhed

Fortrolighed

Alle medarbejdere/konsulenter har som en del af ansættelsen indgået tavshedspligt der sikrer at fortrolig information ikke bliver videregivet. Tavshedspligten gælder både under og efter ansættelse. Tilmed underskriver de relevante medarbejdere erklæring om overholdelse af IT Sikkerhedspolitikken, der yderligere sikrer at oplysninger om systemet og dennes sikkerhedsforhold, medarbejdere, forretningshemmeligheder og oplysninger om forretningsforbindelser forbliver fortrolige.

Styring af aktiver

Fortegnelse over aktiver

Alle systemernes aktiver er identificeret, og der er udarbejdet en fortegnelse over aktiverne. Aktivfortegnelsen er dokumenteret og indeholder relevante beskrivelser af delkomponenter, fysisk og logisk placering samt ejerskab.

Adgangsstyring

Principper for adgangsstyring

Adgange til systemerne tildeles altid med udgangspunkt i "need-to-know"/ "need-to-have" og "least privilege"-principperne, så det tilsikres, at adgange er tildelt brugere med et arbejdsbetinget behov.

Sikker loging med to-faktor autentificering

Der er flere muligheder for systemadgang, alt efter hvilket system vi taler om. Mulighederne spænder fra single sign-on løsning via integration med kundens Microsoft Azure Active Directory til almindelig email/password-autentificering eller via .legal ID.

.legal ID er en egenudviklet login-provider baseret på sikkerhedsprotokollerne OpenID Connect / OAuth2.0 og giver mulighed for at brugeren kan benytte sit .legal ID på tværs af .legal produkter. Tilmed giver .legal ID mulighed for 2-faktor autentifikation.

Rolle- og rettighedsstyring

Adgang til funktionalitet i systemerne styres via en rollebaseret model, hvor en bruger tildeles en række roller, der giver adgang til bestemte dele eller funktioner i systemet. I systemer, hvor der er behov, kan rettighederne yderligere granuleres i forhold til læse og skriveadgang.

Procedure for privilegeret adgang

En medarbejder med behov for adgang til produktionsdata eller produktionsinfrastruktur (privilegeret adgang), skal i tillæg til et arbejdsbetinget behov, have særskilt godkendelse fra direktionen. Medarbejdere med privilegeret adgang anvender altid 2-faktor autentifikation.

Kryptografi

Kryptering

Systemet er en ren browserbaseret løsning. Der er i systemet udelukkende krypteret kommunikationen mellem klienten (browseren) og serveren.

Systemet anvender et SHA-2 SSL certifikat med minimum 2048bit kryptering fra en pålidelig udbyder. Data krypteres, når det bliver gemt i datacenteret, og dekrypteres automatisk, når det skal tilgås.

Fysisk sikring og miljøsikring

Fysisk sikring af lokaler og maskiner

.legals lokaler er til enhver tid aflåst. .legal hoster ikke selv løsninger, hvilket gør at den fysiske sikring først og fremmest vedrører medarbejdernes maskiner. Alle medarbejderes maskiner er krypteret.

Driftssikkerhed

Sikker hosting

Microsoft Azure udgør den overordnede IT platform for systemerne i .legal A/S.

A. Koden opbevares og styres i Azure DevOps.

B. Data opbevares i Azure Storage, Azure SQL samt Azure Cosmos DB i europæiske datacentre i Vesteuropa.

C. Test- og driftmiljøer til applikationerne er ligeledes etableret i Azure.

Systemerne hostes i Microsoft Azure – bl.a. af sikkerhedsmæssige hensyn, da den underliggende platform altid er up-to-date, samt at muligheder for datakryptering, redundans, backup og adgangsstyring generelt er gode.

I forhold til brug af 3. parts services uden for Azure udvælges disse ud fra krav om høj sikkerhedsstandard (f.eks. ISO27001 certificering) samt overholdelse af GDPR. Generelt forsøger vi at mindske behovet for 3. parts services uden for Microsoft Azure.

Data redundans

Produktionsmiljøets datalokation til dokumenter er Vesteuropa. På denne lokation gemmes data i 3 forskellige kopier. I tilfælde af nedbrud skiftes der i Azure platformens opsætning automatisk over på en af de redundante kopier. Systemet anvender Geo Redundant Storage (GRS).

Data backup

PACTIUS samt Privacy foretager natlig backup af data i produktionsmiljøet som lagres i 7 dage. Dertil kommer en månedlig backup, der lagres i 3 måneder. Backup replikeres 3 gange indenfor samme datacenter som databasen kører i (Vesteuropa).

DPA Service kører der continuos backup, der muliggør restore af data til et bestemt tidspunkt. Der kan maksimalt restores 30 dage tilbage i tid. Backup replikeres 3 gange indenfor samme datacenter som databasen kører i (Vesteuropa).

Logning, Monitorering og Alerts

Systemhændelser logges til en centralt systemlog , således er det muligt at spore eventuelle fejl på tværs af komponenter i det samlede system. Det samlede system bliver monitoreret via Dashboards, hvor vi kan følge ressourceforbrug, brugen samt fejl i et samlet overblik. På baggrund af den centraliserede log er der defineret en række alarmer, der håndteres af udviklingsteamet.

High availability
Vi bestræber os på at holde alle vores tjenester tilgængelige 24 timer i døgnet 365 dage om året. Vi releaser løbende nye funktioner og forbedringer, men alle tjenester releases automatisk og de fleste uden nedetid. Hvis en service ikke kan releases uden nedetid, planlægger vi ændringen i henhold til brug, således at så få brugere som muligt påvirkes. Hvis vi ved, at ændringen vil påvirke brugerne, bliver kunden notificeret på forhånd.

Alle vores tjenester hostes på Azure med følgende service-niveau-aftale (SLA):
Webapps SLA: 99,95 %
Cosmos DB SLA: 99,99 %
Azure SQL Server SLA: 99,99 %
SLA for lagerkonti: 99,99 %

Detaljer kan findes her: https://azure.microsoft.com/en-us/support/legal/sla/summary/

Brute force protection
Vores login-udbyder (id.dotlegal.dk) er beskyttet mod brute force-angreb ved at blokere brugeren efter 3 login-forsøg.

Kravene til adgangskoden er:

- Skal indeholde mindst 10 karakterer
- Skal indeholde mindst 5 forskellige tegn
- Må ikke indeholde brugernavnet
- Måske ikke være for almindeligt. (Vi tjekker mod OWASP's SecLists-projekt med 10.000 mest brugte adgangskoder)

Kommunikationssikkerhed

Sikker kommunikation via SSL
Kommunikation mellem browseren og resten af systemet foregår via HTTPS (SHA-2 SSL certifikat med minimum 2048bit kryptering).

Udveksling af data mellem kunderne og systemet foregår enten via SFTP eller indbygget funktionalitet til import og eksport af data, som igen er beskyttet med HTTPS.

Anskaffelse, udvikling og vedligeholdelse af systemer

Udviklingsprocess
Omdrejningspunktet for vores daglige arbejde er vores fælles udviklingsproces, der baserer sig på moderne men velafprøvede metoder som SCRUM og Kanban. Hvert produkt har egen produktejer med ansvar for

planlægning og prioritering samt et fast udviklingsteam med ansvar for udvikling og kvalitetssikring. Dertil kommer support, der taler direkte med produktejeren, udviklingsteamet og kunderne.

Udviklingsprocessen sikrer at vi sparer mundtlig på daglig basis, vender eventuelle udfordringer og hjælper hinanden til effektive løsninger. Vi har flere øjne på de ændringer, vi foretager os, og gør aktivt en indsats for hele tiden at dygtiggøre os og forbedre de systemer, vi arbejder med.

Alle udviklingsteams har erfarne folk om bord for at sikre et højt niveau - også når det gælder sikkerhed.

Kvalitetssikring

Kvalitetssikrende elementer fra den fælles .legal udviklingsproces:

A. Struktureret proces
    i. Alt arbejde, uanset karakter, visualiseres som opgaver i vores opgavestyring. Alle opgaver skal igennem den samme overordnede proces med flere faser der bl.a. dækker kodereview, intern test og accept test.

B. Automatiseret kvalitetssikring
    i. Versionsstyret kode
    ii. Continuos Integration der løbende bygger koden for at sikre integritet
    iii. Automatiserede tests der løbende kører for at minimere regressionsfejl
    iv. Automatiserede deployment pipelines som gør at vi sikkert og med høj sporbarhed kan deploye ny kode til test og produktionsmiljøer.

C. Udviklings-, test- og produktionsmiljø
    i. Dedikerede udviklings, test og produktionsmiljøer for at kunne kvalitetssikre på flere niveauer før ny kode når produktionsmiljøet.

D. Overvågning og alarmering
    i. Vores miljøer er monitoreret således at vi kan sikre høj oppetid og får alarmer om eventuelle fejl eller sårbarheder så hurtigt som muligt.

Leverandørforhold

Leverandøraftaler

A. Der indgås leverandøraftaler med alle kunder der benytter sig systemerne.

B. Eventuelle underleverandører skal leve op til samme sikkerhedsstandard og efterleve samme sikkerhedspolitikker som .legal A/S.

Leverandørkontrol

A. .legal foretager årligt en sikkerhedskontrol af 3. parts serviceleverandører der indgår som en del af det samlede system.

Styring af informationssikkerhedsbrud

Procedure for håndtering af informationssikkerheds nedbrud

Alle sikkerhedsmæssige hændelser eller observerede svagheder rapporteres til direktionen eller den sikkerhedsansvarlige. Så snart der er rapporteret en sikkerhedshændelse eller svaghed sættes følgende aktiviteter i gang:

1. Sikkerhedshændelsen registreres i virksomhedens opgavestyring.

2. I opgavens beskrivelse noteres sikkerhedshændelsen/svagheden i så mange detaljer som muligt, herunder som minimum:
   i. Hvornår hændelsen fandt sted
   ii. Hvad hændelsen konkret gik ud på
   iii. Hvem der har indrapporteret hændelse

3. Hændelsen analyseres herefter med henblik på følgende:
   i. Afgøre hvor omfattende hændelsen er
   ii. Hvilke kunder der er berørt
   iii. Hvad der skal gøres for at enten standse hændelsen eller imødekomme hændelsen i fremtiden f.eks. ved koderettelser

4. Kunder identificeret i punkt 3, informeres herefter omkring hændelsen og konsekvenserne af hændelsen, samt hvilke tiltag der er taget fremadrettet.

5. De tiltag der er blevet besluttet prioriteres og iværksættes

6. Når tiltagene er implementeret lukkes opgaven.

7. Efter problemet er løst beskrives forløbet som et incident i projektets incidentlog. Formålet er at undersøge om der er et underliggende rodproblem, der kan give anledning til yderligere forbedringer eller hjælpe til udbedring af lignende fremtidige problemer.

Overensstemmelse

Procedure for overholdelse af lovgivning

Det påhviler direktionen i .legal A/S, at lovgivningsmæssige sikkerhedskrav overholdes, herunder:

A. Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven)

B. Persondataforordningen (forordning nr. 2016/679)

En gang om året anmoder .legal A/S direktionen advokatvirksomheden Bech-Bruun om at vurdere, om det er sket ændringer i lovgivningen på en måde, så der skal ændres i sikkerhedspolitikken og/eller i systemet. Resultatet af anmodning noteres på bestyrelsesmødet og eventuelle afledte ændringer implementeres.