It-revision

Bilag 6.2

Version: Maj 2022

VISMA

Indhold

Indledning

Dette bilag beskriver processerne for it-revision og dækker følgende i softwaresuiten My Visma: Visma Løn, Visma HR, My Visma app og Datahub.

Information Security

Ansvaret for gennemførsel af it-revision er placeret i afdelingen Information Security, som har reference til den øverste ledelse.

Visma Enterprises Information Security Officer er ansvarlig for:

- Facilitering af intern revision
- Facilitering af eksterne revisioner
- Implementering, vedligeholdelse og løbende forbedring af ledelsessystemet for informationssikkerhed (ISO/IEC 27001:2013).

Informationssikkerhed og revision

Informationssikkerhed er beskrevet i bilag 6.1 – Information Security.

Intern revision

Intern revision gennemføres med planlagte mellemrum for at undersøge, om kravene i den internationale standard ISO/IEC 27001:2013 Information technology – Security techniques – Information management systems – Requirements (herefter ISO 27001) er effektivt implementeret og bliver vedligeholdt.

Rapporter fra intern revision er klassificeret og udleveres ikke til kunder.

Eksterne revisioner

ISO/IEC 27001:2013 certifikat

I 2019 blev Visma's Services ISO/IEC 27001:2013 certificeret og krav om løbende overvågning, måling, analyse og evaluering af ledelsessystemet for informationssikkerhed er implementeret.

ISO/IEC 27001:2013 certifikatet findes på Visma Community og på www.vismaenterprise.dk.

ISAE 3402 type 2

Visma Enterprise får udarbejdet en årlig ISAE 3402 type 2 revisorerklæring af en uafhængig tredjepart. Revisorerklæringen udføres i overensstemmelse med "ISAE 3402 'Assurance Reports on Controls at a Service Organisation', and additional requirements applicable in Denmark".

Kontrolmiljøet er bygget på baggrund af ISO/IEC 27001:2013 annex a, hvor dele af eller hele områder indgår:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationsikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse (compliance).

Revisionserklæringen dækker et år og tilbydes kunder, som har benyttet de reviderede Services helt eller delvist i revisionsperioden.

Revisionserklæringer kan bestilles på webshoppen.

Revisorerklæringer fra leverandører

Leverandørforhold er defineret og implementeret i overensstemmelse med ISO/IEC 27001 a.15. Leverandører med klassificering 'high' leverer en årlig revisorerklæring, som er udarbejdet af en uafhængig tredjepart. Revisorerklæringen udarbejdes efter forskellige standarder afhængig af servicen f.eks. ISAE 3402, ISAE 3000 eller ISRS 4400.

Revisorerklæringer fra leverandørforhold udleveres ikke til kunder.

--