Policy

2022-05-24

Diarienummer: MIUN 2022/1233

Policy för informationssäkerhet

Publicerad: 2022-05-24

Beslutsfattare: Rektor.

Ansvarig funktion: Infrastrukturavdelningen

Handläggare: Helena Wallskog

Beslutsdatum: 2022-05-24

Giltighetstid: Tillsvidare

Senaste översyn: 2022-05-24

Sammanfattning: Informationssäkerhetspolicyn sammanfattar övergripande mål och principer för Mittuniversitetets arbete med informationssäkerhet. Policyn följer Myndigheten för samhällsskydd och beredskaps föreskrifter MSBFS 2020:6-7.

Tidigare versioner:

Dnr 2021/787, 2021-04-06

Dnr 2019/1629, 2019-10-01

Dnr 2018/881, 2018-05-30

Innehållsförteckning

1 Policy för informationssäkerhet 3
1.1 Allmänt 3
1.2 Målsättning 4
1.3 Tillämpningsområde 5
1.4 Principer för informationssäkerhetsarbetet 5
1.5 1.5 Roller och ansvar 5
1.6 Uppföljning och utvärdering 6
1.6.1 Uppföljning 6
1.6.2 Utvärdering 6
1.7 1.7 Utbildning/medvetenhetsträning 6
1.8 Förvaltning av policyn 6

1 Policy för informationssäkerhet

Informationssäkerhetspolicyn för Mittuniversitetet fastställer övergripande mål och inriktning för informationssäkerhet samt anger hur ansvaret i dessa frågor är fördelat. Denna policy utgör grunden i universitetets ledningssystem för informationssäkerhet (LIS). Policyn beskriver ramverket för informationssäkerhet och ska tillsammans med ytterligare styrdokument utgöra ett stöd för verksamheten i det dagliga arbetet. Arbetet med informationssäkerhet utgår från lagar, förordningar, föreskrifter, interna och externa krav samt avtal.

Informationssäkerhet är de åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs.

Policyn tar även hänsyn till dataskyddsförordningen (Europaparlamentets och rådets förordning (EU) 2016/679, GDPR) som utgör en integrerad del av den totala informationssäkerheten.

1.1 Allmänt

Information är en av universitetets viktigaste tillgångar och en förutsättning för att verksamheten ska fungera. Informationen måste därför göras tillgänglig och skyddas från att till exempel läcka ut, förvanskas eller förstöras.

Enligt Myndigheten för samhällsskydd och beredskaps föreskrift om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) ska myndigheten bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav och SS-EN ISO/IEC 27002:2022 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder eller motsvarande.

Figur 1: Ledningssystem för informationssäkerhet

1.2 Målsättning

Målet med informationssäkerhetsarbetet är att:

- Upprätthålla en väl avvägd informationssäkerhet med hänsyn till universitetet, verksamma vid universitetet och allmänhetens behov.
- Säkerställa en rimlig nivå för att skydda informationstillgångar mot olika hot.
- Bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet.
- Bedriva ett systematiskt informationssäkerhetsarbete med hänsyn till lagar, förordningar, föreskrifter, interna och externa krav samt avtal.

1.3 Tillämpningsområde

Informationstillgångar är allt som innehåller information och allt som bär på information. Informationssäkerhet begränsas inte till säkerhet i IT-system utan omfattar information i alla dess former och oavsett hur informationen lagras, bearbetas och kommuniceras. Information kan t ex vara i form av text, ljud, bilder och film, och kan hanteras med stöd av IT, papper eller på annat sätt.

1.4 Principer för informationssäkerhetsarbetet

Grundläggande för informationssäkerhetsarbetet är att det ska bedrivas systematiskt genom kontinuerlig uppföljning, förbättring och vara en integrerad del i organisationens verksamhetsstyrning. Det gäller såväl ansvarsfördelning som riskhantering samt rutiner för planering och budgetarbete.

1.5 1.5 Roller och ansvar

Ansvaret för informationssäkerheten ser ut enligt följande:

- Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret, från ledning ner till enskilda medarbetare.
- Varje medarbetare ska aktivt arbeta för ökad säkerhet, samt påpeka brister till överordnad.
- Enligt Mittuniversitetets riktlinjer för systemförvaltning ansvarar systemgruppsägarna för informationssäkerheten kring verksamhetssystemen.
- Ansvaret för informationssäkerhetsarbetet finns hos Infrastrukturavdelningen (INFRA). I ansvaret ingår att besluta om riktlinjer, rutiner och processer och att stötta ledningen och alla övriga roller som har ett informationssäkerhetsansvar i operativa, taktiska och strategiska frågor.

Andra funktioner som också ger stöd i informationssäkerhetsarbetet är arkiv, juridik, IT och dataskydd.

1.6 Uppföljning och utvärdering

1.6.1 Uppföljning

Uppföljning ska ske regelbundet och vid behov, såsom i samband med verksamhetsuppföljning, omorganisation, förändrade rättsliga krav och inför beslut att låta universitetets information behandlas av en annan statlig myndighet eller en extern aktör.

1.6.2 Utvärdering

Universitetet ska utvärdera hur interna regler, arbetssätt och stöd svarar mot identifierade risker och behov. Utvärderingen sker genom interna kontroller, granskningar, interna och externa revisioner eller motsvarande. Interna regler och arbetssätt ska tydliggöra hur och när utvärdering ska ske.

Informationssäkerhetsarbetet redovisas för ledningsrådet 2 ggr/år och för styrelsen 1 gång/år.

1.7 1.7 Utbildning/medvetenhetsträning

Universitetets medarbetare ska erbjudas relevanta utbildningar utifrån sin funktion/roll i Mittuniversitetets organisation.

Information ska kontinuerligt delges medarbetarna för att öka medvetenheten kring de aktuella risker som finns och hur de bör hanteras.

1.8 Förvaltning av policyn

Universitetsförvaltningen, genom Infrastrukturavdelningen (INFRA), ansvarar för underhåll och uppdatering av