

Policy för informationssäkerhet

2021-04-06

DNR: MIUN 2021/787

Policy för informationssäkerhet

Publicerad: 2021-04-06

Beslutsfattare: Anders Fällström

Handläggare: INFRA, Helena Wallskog

Beslutsdatum: 2021-04-06

Giltighetstid: Till vidare

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

Tidigare versioner:

Dnr 2019/1629, 2019-10-01

Dnr 2018/881, 2018-05-30

Policy för informationssäkerhet

2021-04-06

DNR: MIUN 2021/787

Innehållsförteckning

1. Policy för informationssäkerhet	3
1.1 Allmänt	3
1.2 Målsättning	4
1.3 Tillämpningsområde	4
1.4 Principer för informationssäkerhetsarbetet	4
1.5 Roller och ansvar	5
1.6 Utvärdering och granskningar	5
1.7 Utbildning	5
1.8 Förvaltning av policyn	5

Policy för informationssäkerhet

2021-04-06

DNR: MIUN 2021/787

1. Policy för informationssäkerhet

Informationssäkerhetspolicyen 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). Policyen beskriver ramverket för informationssäkerhet och ska tillsammans med ytterligare styrdokument utgöra ett stöd för verksamheten i det dagliga arbetet.

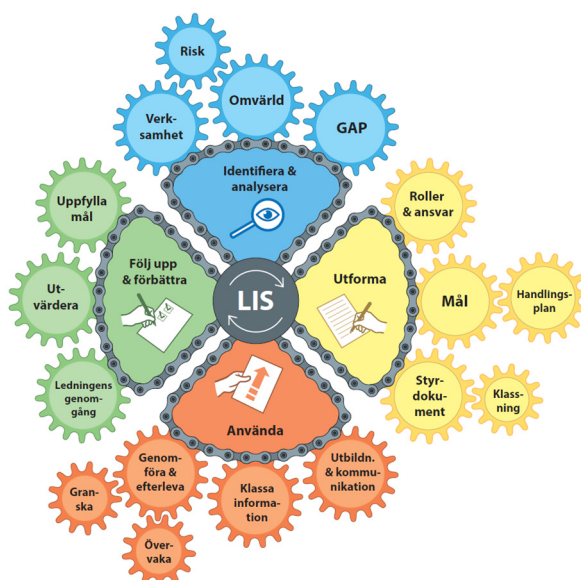
Arbetet med informationssäkerhet utgår från lagar, förordningar, föreskrifter, interna och externa krav samt avtal.

Policyen 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 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder* eller motsvarande.



Figur 1: Ledningssystem för informationssäkerhet, MSB

Policy för informationssäkerhet

2021-04-06

DNR: MIUN 2021/787

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.
- Bygga in de legala krav som ställs på Mittuniversitetet enligt dataskyddsförordningen i det systematiska informationssäkerhetsarbetet.

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 och förbättring, ofta beskrivet genom den s.k. PDCA-cykeln. Med PDCA-cykeln avses processen Plan-Do-Check-Act enligt ledningssystem för informationssäkerhet, SS-ISO/IEC 27001 (Planera – Genomföra – följa upp – Förbättra) samt aktiv dialog med ledning och verksamhet.



Figur 2: Modell för systematiskt arbetssätt med informationssäkerhet

Policy för informationssäkerhet

2021-04-06

DNR: MIUN 2021/787

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.
- Dataskyddsombudets ansvar framgår av MIUN 2018/713
- Ansvaret för informationssäkerhetsarbetet finns hos INFRA-avdelningen enligt beslut av rektor MIUN 2019/583. I ansvaret ingår att besluta om riktlinjer, rutiner, processer etc. samt se till att ett aktivt arbete bedrivs kring frågorna, inklusive att ta fram ett LIS. För arbetet ska det finnas en informationssäkerhetssamordnare på Infrastrukturavdelningen.

Som stöd i informationssäkerhetsarbetet finns funktioner för arkiv, juridik, IT och dataskydd.

1.6 Utvärdering och granskningar

Universitetet ska utvärdera hur interna regler, arbetssätt och stöd svarar mot identifierade risker och behov. Utvärdering 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. 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.

1.7 Utbildning

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

1.8 Förvaltning av policyn

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