Mittuniversitetet
MID SWEDEN UNIVERSITY

Riktlinjer för driftsäkerhet

Publicerad: 2020-11-04

Beslutsfattare: Helena Wallskog

Handläggare: Eva Rodin Svantesson

Beslutsdatum: 2020-11-04

Giltighetstid: Tillsvidare

Ansvarig för förvaltning: Riktlinjerna förvaltas av infrastrukturavdelningen.

Målgrupp: Infrastrukturavdelningen (INFRA).

Sammanfattning: Riktlinjerna sammanfattar universitetets regelverk gällande driftsäkerhet. I samband med upphandling ska kraven i ”kravkatalog för upphandling” beaktas så rätt krav ställs på leverantören utifrån upphandlad tjänst. Riktlinjerna har anpassats utifrån Myndigheten för samhällsskydd och beredskaps föreskrifter MSBFS 2020:6-7.

Innehållsförteckning

1. Riktlinjer för driftsäkerhet

1.1 Driftsrutiner och ansvar

Syfte: Att säkerställa korrekt och säker drift av informationsbehandlingsresurser.

1.1.1 Dokumentation av it-miljön

Följande gäller vid Mittuniversitetet:

Mittuniversitetet ska upprätthålla uppdaterad dokumentation över

a) hård- och mjukvara som används i varje enskilt informationssystem,
b) beroenden mellan olika interna informationssystem respektive beroenden av informationssystem hos externa aktörer,
c) vilka informationssystem som behandlar information som har behov av utökat skydd, och
d) vilka informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag.

1.1.2 Dokumenterade driftsrutiner

Driftrutiner bör dokumenteras och göras tillgängliga för alla systemansvariga/driftansvariga- och tekniskt ansvariga som behöver dem. Dokumenterade rutiner bör finnas för drift av informationsbehandlings- och kommunikationsresurser, såsom uppstarts- och nedtagningsrutin, säkerhetskopiering, underhåll av utrustning, hantering av media, datahall samt hantering av e-post och säkerhet. Driftsrutiner och de dokumenterade rutinerna för systemaktiviteter bör behandlas som formella dokument och ändringar bör godkännas av ledningen. Där så är tekniskt möjligt, bör informationssystem hanteras konsekvent med samma rutiner, verktyg och hjälpmedel.

Följande gäller vid Mittuniversitetet, driftsrutiner bör innefatta specifika instruktioner för:

e) installation och konfiguration av system;
f) automatisk och manuell bearbetning och hantering av information;
g) säkerhetskopiering;
h) fastställd schemaläggning, inklusive beroenden till andra system, tidigaste start för körningar och senaste tidpunkt för slutförande av körningar;
i) instruktioner för hantering av fel eller andra exceptionella omständigheter som kan uppstå under drift, inklusive begränsningar för användningen av systemverktyg;

j) support- och eskaleringskontakter inklusive kontakter för externt stöd vid oväntade funktionella eller tekniska problem;
k) särskilda instruktioner för hantering av utdata och media, användning av särskilda medel eller hantering av konfidentiell utdata inklusive rutiner för säker kassering av utdata från misslyckade körningar;
l) rutiner för återstart och återställande av systemet i händelse av systemfel;
m) hantering av information i transaktionsloggning och systemlogg;
n) rutiner för övervakning.

1.1.3 Ändringshantering

Mittuniversitetet ska säkerställa att förändringar i informationssystem genomförs på ett strukturerat och spårbart sätt.. Formellt ledningsansvar och rutiner ska vara på plats för att säkerställa tillfredsställande styrning av alla ändringar. När ändringar görs bör en granskningslogg som innehåller all relevant information föras.

Mittuniversitetet ska ha interna regler med krav på:

a) vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning
b) hur risker för incidenter och avvikelser i samband med förändring i produktionsmiljön ska identifieras och hanteras
c) hur mjukvara, utan onödigt dröjsmål, ska uppdateras till senaste version
d) hur utbyte eller uppgradering av hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska säkerställas utan onödigt dröjsmål, och
e) hur risker ska hanteras när uppdatering eller uppgradering enligt punkt c och d inte kan genomföras

I övrigt ska följande beaktas vid ändringshantering vid Mittuniversitetet:

f) identifiering och registrering av betydande förändringar;
a) planering och tester av förändringar;
b) bedömning av den potentiella påverkan, inbegripande påverkan på informationssäkerhet, avseende sådana förändringar;
c) formella rutiner för godkännande av föreslagna förändringar;
d) verifiering av att informationssäkerhetskrav är uppfyllda;
e) kommunicera detaljer avseende ändring till alla relevanta personer;
f) fall-back rutiner, inklusive rutiner och ansvar för att avbryta och återställa vid misslyckade ändringar och oförutsedda händelser;
g) tillhandahållande av en ändringsprocess för nödsituationer för att möjliggöra ett snabbt och kontrollerat införande av förändringar som behövs för att hantera en incident.

1.1.4 Kapacitetshantering

Användningen av resurser bör övervakas samt justeras och prognoser av framtida kapacitetskrav bör göras för att säkerställa nödvändig systemprestanda.

Kapacitetskrav bör identifieras med hänsyn tagen till verksamhetsbetydelse för berörda system. Optimering och övervakning av system bör säkerställa och förbättra, där så är nödvändigt, tillgången till, och effektiviteten i systemen. Upptäckande åtgärder bör införas för att indikera problem i god tid. Prognoser för framtida kapacitetskrav bör ta hänsyn till ny verksamhet och systemkrav samt nuvarande och förutspådda trender i organisationens kapacitet för informationsbehandling.

Särskild uppmärksamhet bör ägnas åt resurser med långa ledtider för upphandling eller höga kostnader. Ledningen bör därför övervaka användningen av viktiga systemresurser. De bör identifiera trender i användning, särskilt när det gäller verksamhetsprogram eller systemverktyg.

Ledningen bör använda denna information för att identifiera och undvika potentiella flaskhalsar och beroendet av nyckelpersoner som kan utgöra ett hot mot säkerheten i systemet eller tjänster och planera lämpliga åtgärder.

Att tillhandahålla tillräcklig kapacitet kan uppnås genom att öka kapaciteten eller genom att minska efterfrågan.

1.1.5 Separation av utvecklings-, test- och driftmiljöer

Utvecklings-, test- och driftmiljöer ska vara separerade för att minska risken för obehörig åtkomst eller ändringar i driftmiljön.

Följande gäller vid Mittuniversitetet:

a) regler för överföring av program från utveckling till driftstatus bör definieras och dokumenteras;
b) utvecklingssystem bör hanteras i system eller datorprocessorer och i domäner eller kataloger som inte hanterar produktionssystem;
c) ändringar av produktionssystem och program bör testas i en test- eller mellanstationsmiljö innan överföring till driftsmiljön;
d) annat än i undantagsfall, bör testning inte göras i produktionssystem;
e) kompilatorer, editorer, och andra utvecklingsverktyg eller systemverktyg, bör inte vara tillgängliga från produktionssystem när det inte behövs;
f) användare bör använda olika användarprofiler för produktions- och testsystem och menyer bör visa ett lämpligt identifieringsmeddelande för att minska risken för fel;

g) känslig information bör inte kopieras till testmiljön om inte motsvarande säkerhetsåtgärder som för produktionsmiljön finns för testsystemet
h) utbildning ska inte ske i produktionsmiljön.

1.2 Skydd mot skadlig kod

Syfte: Att säkerställa att information och informationsbehandlingsresurser skyddas mot skadlig kod.

1.2.1 Säkerhetsåtgärder mot skadlig kod

Upptäckande, förebyggande och återställande säkerhetsåtgärder för att skydda mot skadlig kod ska införas i kombination med säkerställande av en lämplig nivå av medvetenhet hos användarna.

Skydd mot skadliga program ska baseras på program för upptäckande av skadlig kod och återställning, informationssäkerhetsmedvetenhet och korrekt åtkomst till system och förändringshantering.

Följande gäller vid Mittuniversitetet:

a) att upprätta en formell regel som förbjuder användningen av icke-auktoriserade program;
b) införa säkerhetsåtgärder som förhindrar eller upptäcker obehöriga program (t.ex. sammanställning över godkända tillämpningar);
c) införa säkerhetsåtgärder som förhindrar eller upptäcker användning av kända eller misstänkta skadliga webbplatser (t.ex. ”svartlistning”);
d) att upprätta en formell regel för att skydda mot risker i samband med erhållande av filer och program från eller via externa nätverk eller annat medium som anger vilka skyddsåtgärder som bör vidtas;
e) att minska sårbarheter som kan utnyttjas av skadlig kod, exempelvis genom hantering av tekniska sårbarheter;
f) genomföra regelbundna översyner av program och datainnehåll för system som stöder verksamhetskritiska processer. Förekomst av icke godkända filer eller obehöriga ändringar bör utredas särskilt;
g) installation och regelbunden uppdatering av program för upptäckt av skadlig kod och återställning som skannar datorer och media som en förebyggande säkerhetsåtgärd eller rutinmässigt. Sökningen som utförs bör omfatta:
    1) alla filer som tas emot via nätverk, eller via någon form av media, avseende förekomst av skadlig kod innan användning;
    2) bifogade filer till e-post och nedladdningar avseende förekomst av skadlig kod innan användning. Genomsökningen bör utföras på flera

ställen, som t.ex. e-postservrar, bärbara datorer och vid anslutning till organisationens nätverk;
3) webbsidor avseende förekomst av skadlig kod;

h) definiera rutiner och ansvar för hantering av system för skydd mot skadlig kod, användarutbildning, rapportering och återhämtning från attacker orsakade av skadlig kod;
i) förbereda lämpliga kontinuitetsplaner för återhämtning från attacker orsakade av skadlig kod, inklusive alla nödvändiga uppgifter och program för säkerhetskopiering och återställning;
j) genomföra rutiner för att regelbundet samla in information, t.ex. prenumerera på nyhetstjänster eller bevaka webbplatser som ger information om ny skadlig kod;
k) genomförande av rutiner för att granska information om skadlig kod och säkerställa att varningsinformation är korrekt och informativ. Verksamhetsansvariga bör se till att kvalificerade källor, t.ex. välrenommerade tidskrifter, tillförlitliga webbplatser eller leverantörer som producerar program till skydd mot skadlig
l) kod används, för att skilja mellan ryktesspridning och verklig skadlig kod. Alla användare bör göras medvetna om problemet med ryktesspridning och lämpliga åtgärder om det inträffar;
m) isolera miljöer där påverkan kan vara katastrofal.

1.3 Säkerhetskopiering

Syfte: Att skydda mot förlust av data.

1.3.1 Säkerhetskopiering av information

Säkerhetskopior av information, program och speglingar av system ska tas och testas regelbundet i enlighet med överenskomna regler för säkerhetskopiering. Säkerhetskopior ska förvaras skilda från produktionsmiljön och skyddas mot skada, obehörig åtkomst och obehörig förändring.

Driftsrutiner bör inbegripa övervakning av säkerhetskopiering, hantera fel vid schemalagda säkerhetskopieringar, samt att säkerställa att säkerhetskopieringen är fullständig enligt reglerna för säkerhetskopiering. Säkerhetskopiering för enskilda system och tjänster bör testas regelbundet för att säkerställa att de uppfyller kraven i kontinuitetsplaner. För kritiska system och tjänster bör säkerhetskopiering omfatta all information, alla program och all data som krävs för att återställa hela systemet i händelse av en katastrof. Lagringstid för viktig verksamhetsinformation bör fastställas med hänsyn till eventuella krav på arkivkopior som behålls permanent.

Vid utformning av en plan för säkerhetskopiering, bör följande beaktas:

a) korrekta och fullständiga register över säkerhetskopior och dokumenterade återställanderutiner utarbetas;
b) omfattning (t.ex. fullständig eller begränsad säkerhetskopiering) och frekvensen av säkerhetskopior bör återspegla kraven i organisationen, säkerhetskraven avseende den aktuella informationen och betydelsen av informationen för den fortsatta driften av organisationen;
c) säkerhetskopierad information bör ges en lämplig nivå av fysiskt och miljömässigt skydd som överensstämmer med kraven för det ordinarie driftstället;
d) i situationer där konfidentialitet är av betydelse, bör säkerhetskopior skyddas genom kryptering.

1.4 Loggning, övervakning och intrångsdetektering

Syfte: Att logga händelser och skapa bevis.

1.4.1 Loggning av händelser

Mittuniversitet ska, för att säkerställa spårbarhet i informationssystem, logga följande säkerhetsrelaterade händelser:

a) obehörig åtkomst och försök till obehörig åtkomst till it-miljö och enskilda informationssystem,
b) förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter,
c) förändringar av behörighet för användare och informationssystem,
d) åtkomst till information som bedömts ha behov av utökat skydd.

1.4.2 Analys av loggar

Mittuniversitet ska analysera innehållet i säkerhetsloggarna för att upptäcka och hantera incidenter och avvikelser. Säkerhetsloggarna ska:

a) möjliggöra utredning av intrång, tekniska fel och brister i säkerheten,
b) utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar, och
c) vara tillgängliga för analys under fastställd bevarandetid.

1.4.3 Skydd av logginformation

Mittuniversitet ska dokumentera hur säkerhetsloggarna ska användas samt var loggningsuppgifter hämtas och lagras, hur de skyddas och hur länge de ska bevaras Loggningsverktyg och logginformation ska skyddas mot manipulation och obehörig åtkomst.

Säkerhetsåtgärder ska syfta till att skydda mot obehöriga ändringar i logginformation och operativa problem med loggningsverktyg inklusive:

a) ändringar av de meddelandetyper som registreras;
b) loggfiler som redigeras eller tas bort;
c) kapaciteteten för lagring av loggdata överskrids, vilket resulterar i antingen att registreringen av händelser upphör eller att tidigare registrerade händelser skrivs över.

1.4.4 Intrångsdetektering

Mittuniversitet ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd.

1.4.5 Realtidsövervakning

Mittuniversitet ska identifiera och hantera behovet av realtidsövervakning av informationssystem.

1.4.6 Synkronisering av tid

Systemklockorna i alla relevanta informationsbehandlingssystem inom en organisation eller säkerhetsdomän ska synkroniseras mot tidstjänsten Swedish Distributed Time Service på www.ntp.se.

1.5 Konfigurering, Säkerhetstester och granskningar

Syfte: Att säkerställa riktigheten hos driftsystem.

1.5.1 Säkerhetskonfigurering

Mittuniversitetet ska, för att skydda informationssystem mot obehörig åtkomst,

a) byta ut förinställda autentiseringsuppgifter,
b) stänga av, ta bort eller blockera systemfunktioner som inte behövs, och,
c) i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet.

1.5.2 Installation av program på driftsystem

Rutiner bör införas för att styra installation av program på driftsystem. Program från leverantör som används i driftsystem bör underhållas på en nivå som stöds av leverantören. Över tid kan programleverantörer upphöra att stödja äldre versioner av

program. Organisationen bör överväga riskerna med att förlita sig på program som inte stöds.

Följande gäller vid Mittuniversitetet:

a) uppdatering av operativsystem, tillämpningar och programbibliotek bör endast utföras av utbildade administratörer efter tillstånd från rätt ledningsfunktion;
b) driftsystem bör endast innehålla godkänd exekverbar kod och inte utvecklingskod eller kompilatorer;
c) tillämpningar och operativsystem bör endast införas efter omfattande och lyckade tester. Testerna bör täcka användbarhet, säkerhet, effekter på andra system och användarvänlighet och bör utföras på separata system. Det bör säkerställas att alla motsvarande programs källkodsbibliotek har uppdaterats;
d) ett system för konfigurationsstyrning bör användas för att styra alla införda program och systemdokumentationen;
e) en plan för återställning bör finnas innan förändringar genomförs;
f) en granskningslogg bör upprätthållas för alla uppdateringar i bibliotek för driftsystems;
g) tidigare versioner av program bör bibehållas som en kompletterande åtgärd;
h) gamla versioner av program bör arkiveras, tillsammans med all information och de parametrar som krävs, rutiner, konfigurationsinformation och supportprogram så länge data lagras i arkivet.

1.5.3 Säkerhetstester och granskningar

Mittuniversitetet ska säkerställa att säkerhetstester och granskningar möjliggör identifiering av sårbarheter. Myndigheten ska ha interna regler för hur kontroll görs av att

a) informationssystemen är uppdaterade,
b) valda säkerhetsåtgärder är införda på korrekt sätt, och
c) genomförda säkerhetskonfigurationer är tillräckliga.

1.6 Hantering av tekniska sårbarheter

Syfte: Att förhindra utnyttjande av tekniska sårbarheter.

1.6.1 Hantering av tekniska sårbarheter

Information om tekniska sårbarheter i de informationssystem som används bör erhållas i tid, organisationens exponering för sådana sårbarheter analyseras och

lämpliga åtgärder vidtas för att behandla den tillhörande risken. Lämpliga, snabba åtgärder bör vidtas vid identifiering av potentiella tekniska sårbarheter.

Följande gäller vid Mittuniversitetet:

a) organisationen bör fastställa roller och ansvar för hantering av tekniska sårbarheter, inkluderande övervakning av sårbarheter, riskbedömning av sårbarheter, uppdateringar av system och övervakning av tillgångar samt för den samordning som krävs;
b) informationsresurser som används för att identifiera relevanta tekniska sårbarheter och upprätthålla medvetenheten om dem, bör identifieras för program och annan teknik (baserat på inventering av tillgångar. Dessa informationsresurser bör uppdateras när inventering av tillgångar förändras eller när andra nya eller användbara resurser identifieras;
c) en tidsgräns bör definieras för agerande på information om potentiellt relevanta tekniska sårbarheter;
d) när en potentiell teknisk sårbarhet har upptäckts bör organisationen analysera riskerna och identifiera åtgärder som bör vidtas. Sådana åtgärder kan inkludera uppdateringar av sårbara system eller vidtagande av andra säkerhetsåtgärder;
e) beroende på hur snabbt en teknisk sårbarhet behöver åtgärdas bör de åtgärder som vidtas utföras i enlighet med de säkerhetsåtgärder som avser förändringshantering eller genom att följa rutiner för incidenthantering;
f) om det finns en uppdatering från en legitim källa bör risker i samband med installation av uppdateringen bedömas (riskerna med sårbarheten bör jämföras med risken för installation av uppdateringen);
g) uppdateringar bör testas och utvärderas innan de installeras för att säkerställa att de är verkningsfulla och inte leder till effekter som inte kan tolereras. Om ingen uppdatering är tillgänglig, bör andra säkerhetsåtgärder övervägas, såsom att:
    1) stänga av tjänster eller funktioner relaterade till sårbarheten;
    2) anpassa eller lägga till säkerhetsåtgärder för åtkomst, exempelvis i brandväggar eller vid gräns för
        i. nätverk (se 13.1);
    3) öka övervakningen för att upptäcka verkliga attacker;
    4) öka medvetenheten om sårbarheten;
h) en logg bör hållas för alla vidtagna åtgärder;
i) processen för hantering av tekniska sårbarheter bör regelbundet övervakas och utvärderas för att säkerställa dess effektivitet och verkan;
j) system med hög risk bör åtgärdas först;
k) en verkningsfull process för hantering av tekniska sårbarheter bör samordnas med incidenthantering när det gäller att ge underlag om sårbarheter till

funktionen för incidenthantering och för att ta fram tekniska åtgärder som kan användas om en incident inträffar;

l) definiera en rutin för att hantera situationen då sårbarheter har upptäckts men det saknas lämplig motåtgärd. I denna situation bör organisationen utvärdera risker avseende känd sårbarhet och definiera lämpliga upptäckande och korrigerande åtgärder.

1.6.2 Restriktioner för installation av program

Regler för programinstallationer som utförs av användare bör upprättas och införas. Organisationen bör definiera och verkställa regler för vilka typer av program en användare kan installera.

1.7 Redundans och återställning

Mittuniversitetet ska, för att säkerställa tillgänglighet till information och informationssystem vid incidenter och avvikelser,

a) ha interna regler för återställning av produktionsmiljön i sin helhet och för enskilda informationssystem,
b) öva återställning av informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och
c) placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen.

1.8 Överväganden gällande revision av informationssystem

Syfte: Att minimera revisionsverksamhetens påverkan på driftsystem.

1.8.1 Revisionskontroller för informationssystem

Revisionskrav och revisionsaktiviteter som omfattar verifiering av status på driftsystem bör planeras noggrant och godkännas för att minimera störningar i verksamhetsprocesser.

Följande gäller vid Mittuniversitetet:

a) krav på åtkomst till system och data bör avtalas med lämplig ledningsfunktion;
b) omfattningen av tekniska revisionsaktiviteter bör överenskommas och styras;
c) revisionsaktiviteter bör begränsas till skrivskyddad åtkomst av program och data;
d) annan åtkomst än skrivskyddad bör endast tillåtas på kopior av systemfiler som bör raderas när granskningen är klar eller ges lämpligt skydd om det finns en skyldighet att spara sådana filer som dokumenterad information;
e) krav för särskild eller ytterligare bearbetning bör identifieras och avtalas;
f) revisionstester som kan påverka tillgänglighet bör köras utanför kontorstid;
g) all åtkomst bör övervakas och loggas för att producera en spårbarhetskedja.