ALGTEKST-TERVIKTEKST

Kinnitatud kantsleri korraldusega nr 108

Redaktsiooni jõustumise kuupäev: 02.05.2024

Pöördumiste, intsidentide, sündmuste ja probleemide haldus

Sisukord

[1 Üldine 2](#_Toc163738641)

[2 Pöördumiste tüübid 2](#_Toc163738642)

[3 Pöördumiste lahendamine 4](#_Toc163738643)

[3.1 Pöördumiste kanalid ja nende registreerimine 4](#_Toc163738644)

[3.2 Pöördumistele reageerimine ja esimese vastuse andmine 5](#_Toc163738645)

[3.3 Pöördumise lahendamine ja lõpetamine 5](#_Toc163738646)

[4 Intsidendihalduse portsessi kirjeldus 5](#_Toc163738647)

[4.1 Intsidendi avastamine 6](#_Toc163738648)

[4.2 Intsidendile reageerimine ja prioriteetide määramine 6](#_Toc163738649)

[4.3 Intsidendi lahendamine 8](#_Toc163738650)

[4.4 Intsidendi sulgemine ja järel analüüs 8](#_Toc163738651)

[5 Probleemihaldus 9](#_Toc163738652)

[5.1 Probleemi kirjeldamine 9](#_Toc163738653)

[5.2 Probleemi kirjeldamine ja analüüs 9](#_Toc163738654)

[5.3 Probleemi lahendamine ja sulgemine 10](#_Toc163738655)

[6 Järelevalve 10](#_Toc163738656)

# Üldine

Pöördumiste, sündmuste ja intsidentide halduse protsesside (edaspidi protsess) eesmärgiks on tagada kasutajatele teenus kokkulepitud tingimusel ning vigade esinemisel kõrvaldada need esimesel võimalusel.

Protsess koondab enda alla pöördumiste, intsidentide ja sündmuste määratlemise, registreerimise, diagnoosimise, lahendamise ja sulgemise tegevused, et tagada võimalikult kiire ja kvaliteetne pöördumise lahendamine.

# Pöördumiste tüübid

**Pöördumine** - pöördumiseks nimetame kõik võimalike esitatud päringuid, nõu küsimisi, soove, teavitusi, mida ei ole veel liigitatud konkreetse tüübi järgi.

**Pöörduja** - kasutaja, ülikoolis töötav isik, üliõpilane, partner jt, kes kasutavad ülikooli poolt pakutavaid teenuseid või infosüsteeme.

**Sündmused** – monitooringu süsteemi poolt avastatud teenuse komponentide rikete või hoiatuste teavitused, mis võivad põhjustada andmete konfidentsiaalsuse, terviklikkuse või käideldavuse kadu. Sündmustest saavad pöördumised.

**Pöördumiste tüübid on järgmised**:

* **Intsident** – planeerimata sündmus, mis häirib või vähendab teenuse kvaliteeti või tekitab teenuse katkestuse ning millega kaasneb või tekib oluline oht andmete ja/või muude varade käideldavuse, tervikluse ja/või konfidentsiaalsuse kaoks.
	+ **Küberturvalise intsident (küberintsident)** – intsidendi eriliik, mille raames on toimunud edukas või edutu katse või rünne mingit IT vara hävitada, muuta, blokeerida, varastada või saada lubamatu juurdepääsu või kasutada seda lubamatult.
	+ **Andmekaitse intsident** - intsidendi eriliik, mille raames toimub edastatavate, salvestatud või muul viisil töödeldavate isikuandmete turvalisuse rikkumine, juhusliku või ebaseaduslik hävitamine, kaotsiminek, kättesaamatuks muutumine, lubamatu juurdepääs või andmete loata avalikuks saamine.
	+ **Esitlustehnika intsident** – intsidendi eriliik, mille raames on tuvastatud esitlustehnika lahenduse mitte ootuspärane toimimine või rike.
* **Teenuse taotlus** (service request) - ehk teenindussoov on soov saada informatsiooni, nõu, teenust, ligipääsu või midagi uut.
	+ **IT vahendite hankimine** – teenuse taotluse vorm, mille eesmärgiks on hankida sobiv tarkvara või riistvara komponent.
	+ **Juurdepääsuõigused –** teenuse taotluse vorm, mille eesmärgiks saamaks ligi infosüsteemile või muule infotehnoloogilisele varale.
	+ **Kasutajakontode tellimused –** teenuse taotluse vorm(id), mille kaudu saab esitada tellimusi seoses kasutajakontodega.
	+ **Arvuti- ja õppetöökoht** - teenuse taotlus vorm(id), mille kaudu saab tellida erinevaid töid seoses arvutitöökohaga, sh arvutiklassid ja auditooriumite arvutid (operatsioonisüsteemid, ühistöölahendused, e-post ja listid, printerid).
	+ **Mobiil- ja lauatelefonidega seotud tellimused** – teenuse taotluse vorm(id), mille kaudu saab tellida erinevaid toiminguid seoses mobiili- ja lauatelefoniga.
	+ **Võrk- ja serverid** – teenuse taotluse vorm(id), mille kaudu saab tellida erinevaid võrguseadistusi ja serveritega seotud teenuseid.
	+ **Esitlustehnika lahendused**- teenuse taotluse vorm, mille kaudu saab tellida erinevaid esitlustehnikalahendusi auditooriumites kui ka nõupidamis ruumidesse.
	+ **Sündmuste AV tehniline teenindamine** – teenuse taotluse vorm, mille kaudu saab tellida sündmuse tehnilist teenindamist (audio- ja videolahendused)
	+ **IT arendusettepanek** - on ettepanek IT alaseks arendustööks, mida saavad teha kõik ülikooli liikmeskonna liikmed.
* **Probleem** - ühe või enama intsidendi tekkepõhjus, teenuse kvaliteedi langus või oht intsidentide tekkimisele ja teenuse kvaliteedi langusele.
	+ **Tuntud viga**- probleem, mille tekkepõhjus ja ajutine ja/või lõplik lahendus on teada ning need on ka dokumenteeritud.

**Pöördumistega seotud ajad on järgmised:**

**Reageerimisaeg** on aeg, mille jooksul tuleb reageerida pöördumisele ehk aeg mil pöördumine vaadatakse läbi kasutajatoe töötaja poolt, pöördumine klassifitseeritakse ja määratakse prioriteet ning lahendaja (*assignee*).

Reageerimisajad tööajal erinevates kanalites

* E-maili või JIRA keskkonna laekunud pöördumistele reageerimisaeg on 180 minutit.
* Telefoni teel laekuvate pöördumisele reageerimisaeg on kuni 5 minutit.

**Esimese vastuse aeg** (*First Response Time*) on aeg, mis kulub pöördumise esitamisest kuni esimese vastuseni. Esimese vastuse aeg mõõdab aega, mis kulub teenindusagendil (kasutajatoe töötajal) kliendi päringule vastamiseks pärast selle esitamist. Esimese vastuse aeg on kuni 24h kõikide pöördumiste puhul ehk kuni kolm tööpäeva.

**Lahendamise aeg** (*Resolution Time*) on aeg, mis kulub pöördumise lahendamiseks või küsimusele vastamiseks. Lahendamise aeg sõltub pöördumise keerukusest ja prioriteedist.

# Pöördumiste lahendamine



Joonis 1 Pöördumiste lahendamine

## Pöördumiste kanalid ja nende registreerimine

Kasutajad saavad pöörduda järgnevate kanalite kaudu: JIRA tugiportaal, e-mail, telefon, tulles kohapeale (*walk-in*). Kõik pöördumised kasutajate poolt tuleb registreerida JIRA piletihalduskeskkonda. Pöördumised, mis esitatakse JIRA tugiportaali või e-maili kaudu aadressile helpdesk@taltech.ee registreeritakse automaatselt. Telefoni teel ja kohapealsed pöördumised registreeritakse asutajatoe spetsialisti poolt.

Pöördumiste puhul registreeritakse alati isik (nimi või kasutajanimi) ja pöördumise sisu JIRA piletihalduskeskkonda.

Pöördumistena registreeritakse ka monitooringu kaudu tulevad sündmused.

## Pöördumistele reageerimine ja esimese vastuse andmine

Tööajal reageerimine pöördumistele algab registreerimise hetkest. Töövälisel ajal registreeritud piletite reageerimiseaeg algab järgneval tööpäeval.

Kõigile registreeritud pöördumistele reageerib IT kasutajatoe töötaja tööajal 180 minuti jooksul ja teostab **esmase analüüsi** ja/või **tõrke tuvastuse**. Kasutajatoe töötaja klassifitseerib pöördumise ning määrab pöördumisele prioriteedi ja lahendaja (*assignee*).

Kasutajatoe spetsialist annab tööajal omalt poolt 24h jooksul ehk kolme tööpäeva jooksul esimese vastuse pöördujale temaga seotud pöördumise osas.

Tabel 1 Pöördumise prioriteedi määramine

|  |  |
| --- | --- |
|  | **Mõju** |
| Mõjutatud enam kui 50 kasutajat | Mõjutatud 10 kuni 50 kasutajat | Mõjutatud kuni 10 kasutajat | Mõjutatud üks kasutaja |
| **Kiireloomulisus** | Väga kiire | Kriitiline | Kõrge | Keskmine | Keskmine |
| Kiire | Kõrge | Keskmine | Keskmine | Madal |
| Keskmine | Keskmine | Keskmine | Madal | Madal |
| Madal | Keskmine | Madal | Madal | Madal |

## Pöördumise lahendamine ja lõpetamine

Võimaluse korral lahendab kasutajatugi pöördumise ise ja kui endal ei ole võimalust lahendada, siis suunab pileti lahendamiseks kokkulepitud isikule tulenevalt pöördumise tüübist ja sisust. Sealhulgas kasutajatoe spetsialist enne suunamist on teinud **esmase analüüsi**, vajadusel küsinud kasutaja käest täiendavat informatsiooni ning pöördumisele lisanud tõrke tuvastuse kirjelduse.

Pöördumised, mis lahendatakse mõne partneri poolt, on pöördumise lahendamise eest vastutav pileti registreerinud ülikooli kontaktisik kuni pöördumise sulgemiseni.

Pöördumiste lahendamine toimub prioriteetide. Pöördumised lahendatakse nii kiiresti kui võimalik. Kõik pöördumise **lahendamisel tehtud toimingud dokumenteeritakse tegevuse hetkel JIRA keskkonnas** või esimesel võimalusel pärast seda detailsusega, mis võimaldab hilisemal ülevaatusel mõista tehtu olemust.

Pöördumise märgib töövahendis lahendatuks pöördumise lahendaja koheselt pärast selle lahendamist. Pöördumise lahendatud lugemise eelduseks on see, et kasutaja mure on lahendatud ning see on kasutajatoe töötaja poolt üle kinnitatud.

Pöördumise lahendamisel dokumenteeritakse selle lõplik lahenduskäik. Juhul kui pöördumise on lahenduse märkimine on jäänud töövahendis tegemata võib pöördumise suletuks märkida kasutajatoe juht.

# Intsidendihalduse portsessi kirjeldus

**Intsidentide koordinaatorid** on IT osakonna talituste juhid, kelle ülesandeks on tagada, et kõrge ja kriitilise prioriteediga intsident saaks tulemuslikult lahendatud ning vastutab kommunikatsiooni korraldamise eest. Intsidendid koordinaatorid järjekorras on:

* IT kasutajatoe juht (*vaikimisi*);
* IT taristu talituse juht;
* IT arendustalituse juht;
* Infoturbe juht (vaikimisi infoturbega seotud intsidentide puhul)
* IT osakonna juht.

## Intsidendi avastamine

* Intsidendi avastamine erinevates rollides
	+ kasutaja, kes tuvastab, et mõni infosüsteem või mõni muu infotehnoloogiline vara ei toimi ootuste päraselt. Kasutaja teavitab intsidendist esimesel võimalusel erinevate pöördumiskanalite kaudu IT kasutajatuge ning sh võtab võimalusel tarvitusele õiguspärased abinõud intsidendiga kaasneva kahju vähendamiseks või selle mõju laienemise vältimiseks.
	+ Monitooringu seire sündmus, mis teavitab kasutajatuge võimalikust intsidendist.
	+ IT osakonna töötaja, kes tuvastab, et mõni infosüsteem või mõni muu infotehnoloogiline vara ei toimi ootuste päraselt. IT osakonna töötaja teavitab esimesel võimalusel intsidendist oma vahetut juhti ja/või IT kasutajatuge.

## Intsidendile reageerimine ja prioriteetide määramine

* **Stsenaarium 1** - kui intsidendi avastab kasutaja ja annab sellest teada kasutajatoele või kasutajatoe töötaja ise avastab intsidendi
	+ Kasutaja avastatud ja raporteeritud intsidendid kui ka tehnilised monitooringu sündmused registreeritakse IT kasutajatoes.
	+ Intsidendile reageerimine toimub sarnaselt pöördumiste lahendamisele ehk kõige pealt pöördumine klassifitseeritakse intsidendiks, määratakse lahendaja (assignee) ja seotakse pöördumine konkreetse infosüsteemi või muu infotehnoloogilise varaga.
	+ Lahendaja teeb esmase analüüsi ja/või tõrke tuvastuse (vajadusel küsib täiendavat informatsiooni kasutajalt).
	+ Lahendaja võtab ühendust vastava infosüsteemi süsteemiadministraatoriga (või muu seotud osapoolega), et ta omalt poolt kontrolliks lahenduse toimimist.
	+ Kui intsident saab kinnitud, siis lahendaja määrab intsidendile prioriteedi.
		- Kui tegemist on madala kuni keskmise prioriteediga intsidendiga, siis lahendajaks jääb kasutajatoe töötaja. Kui kasutajatugi saab intsidendi ise lahendada, siis intsidenti ei suunata edasi ja lahendaja lahendab intsidendi ise ära. Lahendaja informeerib infosüsteemi äriprojektijuhti ja peakasutajat intsidendist või vastavat infotehnoloogilise vara omaniku.
		- Kui tegemist on kõrge või kriitilise prioriteediga intsidendiga, siis määratakse koordinaatoriks kasutajatoe juht (kui kasutajatoe juht ei saa reageerida, siis intsidenti lahendamine liigub intsidendi koordinaatorite nimekirja pidi edasi).
	+ Kui sama intsidendi kohta on rohkem pöördumisi, siis need seotakse kasutajatoe töötaja poolt peamise intsidendi lahendamise piletiga.
* **Stsenaarium 2** – kui intsidendi avastab IT osakonna töötaja:
	+ Intsidendi avastanud töötaja teavitab esimesel võimalusel oma vahetut juhti ja/või IT kasutajatuge
	+ Vahetujuht koos töötajaga teeb analüüsi. Vahetu juht võtab ühendust süsteemihalduriga (või muu seotud osapoolega), et ta omalt poolt kontrolliks lahenduse toimimist.
	+ Kui intsident saab kinnitud, siis vahetujuht määrab intsidendile prioriteedi.
		- Kui tegemist madala kuni keskmise prioriteediga, siis see registreeritakse IT kasutajatoes ning suunatakse lahendamiseks isikule, kes saab selle ära lahendada. Lahendaja informeerib infosüsteemi äriprojektijuhti ja peakasutajat intsidendist või vastavat infotehnoloogilise vara omaniku.
		- Kui tegemist on kõrge või kriitilise prioriteediga intsidendiga, siis koordinaatoriks asub vahetu juht. Kui see intsident nõuab vahetu juhi enda tugevat sekkumist asja lahendamisse, siis delegeeritakse koordineerimine mõnele teisele kättesaadavale vahetule juhile (intsidendi koordinaatorile). Intsidendi koordinaator registreerib intsidendi kasutajatoes ja teavitab kasutajatuge sellest ning informeerib infosüsteemi äriprojektijuhti ja peakasutajat intsidendist või vastavat infotehnoloogilise vara omaniku.
	+ Kui sama intsidendi kohta on rohkem pöördumisi, siis need seotakse kasutajatoe töötaja poolt peamise intsidendi lahendamise piletiga.
* **Stsenaarium 3** – kui intsidendi avastab talituse juht või IT osakonna juht.
	+ Juht teeb esmase analüüsi.
	+ Juht võtab ühendust süsteemihalduriga (või muu seotud osapoolega), et ta omalt poolt kontrolliks lahenduse toimimist.
	+ Kui intsident saab kinnitatud, siis juht määrab intsidendile prioriteedi.
		- Kui tegemist madala kuni keskmise prioriteediga, siis see registreeritakse IT kasutajatoes ning suunatakse lahendamiseks isikule, kes saab selle ära lahendada. Lahendaja informeerib infosüsteemi äriprojektijuhti ja peakasutajat intsidendist või vastavat infotehnoloogilise vara omaniku.
		- Kui tegemist on kõrge või kriitilise prioriteediga intsidendiga, siis intsidendi koordinaatoriks asub juht. Kui see intsident nõuab juhi enda tugevat sekkumist asja lahendamisse, siis delegeeritakse koordineerimine mõnele teisele kättesaadavale juhile (intsidendi koordinaatorile). Intsidendi koordinaator registreerib intsidendi kasutajatoes ja teavitab kasutajatuge sellest ning informeerib infosüsteemi äriprojektijuhti ja peakasutajat intsidendist või vastavat infotehnoloogilise vara omaniku.
	+ Kui sama intsidendi kohta on rohkem pöördumisi, siis need seotakse kasutajatoe töötaja poolt peamise intsidendi lahendamise piletiga.

Tabel 3 Intsidendi prioriteedi määramine

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Mõjutatud enam kui 50 kasutajat | Mõjutatud 10 kuni 50 kasutajat | Mõjutatud kuni 10 kasutajat | Mõjutatud üks kasutaja |
| Infosüsteemi kriitilisus – 3 | Kriitiline | Kõrge | Keskmine | Keskmine |
| Infosüsteemi kriitilisus – 2 | Kõrge | Keskmine | Keskmine | Madal |
| Infosüsteemi kriitilisus – 1 | Keskmine | Keskmine | Madal | Madal |
| Infosüsteemi kriitilisus – 0 | Keskmine | Madal | Madal | Madal |

Intsidendi prioriteet on järgmiste muutujate korrutis:

* Infosüsteemi kriitilisus (kirjeldatud JIRA teenuste kataloogis)
* Pöördumise ulatus - määratakse pöördumise registreerija poolt teadaoleva info põhjal, vastavalt mõjutatud kasutajate ulatuse järgi.

Kui intsident on põhjustanud rahalise kahju on see vähemalt **kõrge** prioriteediga**.**

**Infoturbe intsident on alati vähemalt kõrge prioriteediga**. Kui on tuvastatud mõju teenus(t)ele või lahendaja on teinud peale olukorra hindamist sellekohase otsuse, eskaleeritakse juhtum kriitiliseks.

## Intsidendi lahendamine

* Madala või keskmise tasemega intsidentide puhul intsidendi lahendaja või kõrge või kriitilise taseme puhul intsidendi koordinaator tekitab ühise infovälja erinevate osapooltega intsidendi lahendamiseks või asjaoludest informeerimiseks kasutades antud olukorras sobilikke infokanaleid.
* Intsidendi lahendaja või intsidendi koordinaator tagavad, et intsidendi lahendamiseks vajalikud osapooled saaksid intsidenti lahendada vastavalt lahendusajale.
* Intsidendi lahendaja või intsidendi koordinaator korraldavad vajadusel teavitused mõjutatud kasutajatele. Teavitus peab sisaldama informeeritakse intsidendist, selle ulatusest ja prognoositavast lahendusajast. Üldjuhul teavitused lähevad välja IT kasutajatoe poolt.
* Kasutajatele edastatavad teavitused on kirjutatud korrektses eesti ja inglise keeles ja sisaldavad kasutajatele piisavat informatsiooni intsidendi ulatuse kohta, juhiseid edasiseks käitumiseks ja prognoositavat lahendusaega. Intsidendi lahendaja või intsidendi koordinaator valivad sobilikud kanalid vastavalt intsidendile.
* Juhul kui intsidendist on vaja teavitada laiemat avalikust, siis intsidendi koordinaator kooskõlastab sõnumid turundus- ja kommunikatsiooniosakonnaga ning nemad korraldavad avalikuse teavitamise.
* Infoturbeintsidendi puhul teavitatakse infoturbejuhti, kes otsustab partnerite teavitamise vajaduse ja ulatuse.

Tabel 5 Intsidentide lahendusajad

|  |  |
| --- | --- |
| Prioriteet | Intsidendi lahendusaeg tööajal  |
| Kriitiline | 4h |
| Kõrge | 8h |
| Keskmine | 24h |
| Madal | 48h |

## Intsidendi sulgemine ja järel analüüs

* Intsident suletakse kui pilet on lahendatud või kui piletit ei ole võimalik lahendada. Intsidendi sulgemisel dokumenteeritakse sulgemise põhjus vastavas piletis.
* Intsidendi lahendaja koostab hiljemalt 5 tööpäeva jooksul pärast intsidendi algust intsidendi raporti JIRA töövahendis.
* Infoturbe juht vaatab intsidendid ja nende lahenduskäigud üle ning teeb oma poolsed ettepanekud edaspidiseks.
* Intsidente järel analüüsiks tuleb senised intsidendid klassifitseerida järgnevate kategooriate alusel:
	+ **Personaliviga (personalirisk)** - põhjuseks inimesed, nt vargused, lubamatud tegevused (pettused, väärteod, tööseadusandluse rikkumine, töötajate organiseeritud tegevus), võtmetöötajate puudus või kaotus, töötajate tegevus või tegevusetus, mis avalikustades võib kaasa tuua mainekahju, töötaja tegevus teadmatusest (puudulikud koolitused).
	+ **Protsessiviga (protsessirisk)** - põhjuseks erinevad puudused protsessides, puudused dokumentatsioonis ja lepingutes, , seadusandlusele mittevastamine, ülikooli Sise regulatsioonide aegumine.
	+ **Süsteemiviga (süsteemirisk)** - põhjuseks IT või muud süsteemid - nt investeeringud tehnoloogiasse või nende puudumine, arendamine ja rakendamine, võimsuse ja mahu arvestuse puudumine, süsteemi häired ja katkestused, turvalisus, infoturve.
	+ **Väline viga (välisrisk)**, põhjuseks välised tegurid – kriminaalne tegevus, välised teenusepakkujad, kohtuasjad, pandeemiad, katastroofid, infrastruktuuri häired, poliitiline risk, järelevalve, kohalolek teistes riikides või distantsilt piiriülestele klientidele teenuse osutamine, tooteid ja teenuseid tarbivate klientide risk, klientide hooletusest või käitumisest tingitud riskid.
	+ **Füüsiline viga (füüsiline risk)**, põhjuseks füüsilised tegurid – hoonete ja seadmetega seotud füüsilised ohud, ehituslikud jm keskkondlikud (nt trellid, tarad), mehaanilised (nt lukud, sprinklerid), elektroonilised (signalisatsioon, videovalve), protseduurilised (nt inimvalve). Pöördumise uurimine, diagnoosimine ja lahendamine.

# Probleemihaldus

Probleemihalduse eesmärgiks on infosüsteemidega seotud probleemidele, vähendades intsidentide ja probleemide mõju teenustele, sh:

* Ennetavad tegevused vältimaks intsidentide ja probleemide tekkimist;
* Meetmed vähendamaks korduvate intsidentide tekkimist;
* Vähendada vältimatute intsidentide mõju;
* Mõista intsidentide algpõhjust.

Intsidentide ennetamiseks ja/või mõju vähendamiseks tegeleb infosüsteemi äriprojektijuht või muu infotehnoloogilise vara omanik ennetavalt probleemide defineerimisega läbi teenuse seire, jooksva intsidentide analüüsi ja riskianalüüsi.

Probleemihalduse protsessi juhib probleemihaldur, kes vastutab probleemihalduse tulemuslikkuse ja optimaalse toimimise eest,

## Probleemi kirjeldamine

Sama tekkepõhjusega intsidentide tuvastamisel defineerib avastaja probleemi JIRAs probleemi piletina ning suunatakse infosüsteemi eest vastutavale IT projektijuhile. Intsidendikirjet ei tohi muuta probleemiks, vaid sellest tuleb defineerida probleemikirje. Probleem peab olema defineeritud võimalikult konkreetselt ning detailselt tuleb kirja tekkinud probleem ja selle ulatus, määrata esialgne tekkepõhjuse liik ja prioriteet.

Probleemidel on neli prioriteedi taset: kriitiline, kõrge, keskmine ja madal. Probleemi prioriteedi määramisel lähtutakse teenuse ärikriitilisusest, probleemi põhjustavate intsidentide prioriteedist ning mõjust äriprotsessile. Vajadusel probleemi lõpliku prioriteedi lepivad kokku IT projektijuht ja infosüsteemi äriprojektijuht/peakasutaja. Probleemi mõjust tulenevatest prioriteetidest aitavad aru saada tegurid, mis väljenduvad järgnevalt:

|  |  |  |
| --- | --- | --- |
| Prioriteet  | Probleemi mõju | Maksimaalne lahendusaeg |
| Kriitiline | Olulise infosüsteemi põhifunktsionaalsus ei tööta, toob kaasa pidevaid teenuse katkestusi või andmekadusid | < 1 kuu |
| Kõrge | Olulise infosüsteemi kõrval funktsionaalsus ei tööta, võib kaasa tuua korduvaid katkestusi, äriprotsessi toimimine on häiritud, kuid mitte takistatud. | < 3 kuud |
| Keskmine | Olulise infosüsteemi kõrval funktsionaalsus ei tööta, võib kaasa tuua katkestusi, äriprotsessi toimimine on osaliselt häiritud ja tekitab ebamugavusi, kuid töö tegemine ei ole takistatud. | < 6 kuud |
| Madal | Probleem ei avalda olulist mõju infosüsteemidele ega mõjuta äriprotsesse. | > 6kuud |

## Probleemi kirjeldamine ja analüüs

* Kui probleem on algatatud ning suunatud IT projektijuhile, siis tema ülesanne on tegeleda probleemi kirjelduse ülevaatuse ning detailsemaks kirjutamisega. Juhul kui probleemi detailide uurimisel selgub, et tegemist ei ole probleemiga, siis probleem tuleb sulgeda. Ebatäpse probleemi defineerimise korral, tuleb probleemi kirjeldust täpsustada lahendaja poolt.
* Probleemi uurimise käigus tuvastatakse probleemi põhjustajad ja leitakse ajutised lahendused intsidendi lahendamiseks, vähendamaks probleemi mõju, kuniks vajalikud parandused/muudatused on rakendatud. Ajutise lahenduse väljatöötamise käigus planeerib probleemi lahendaja tegevused, mida tuleb teha probleemi mõju kiireks ja ajutiseks vähendamiseks või kõrvaldamiseks. IT projektijuht koordineerib ajutise lahenduse realiseerimise vastavalt planeeritud tegevustele ja ajakavale.
* Eelnevalt kogutud info alusel peab olema selge, millises infosüsteemi komponendis on probleemi tekkepõhjus, et lahendusmeeskonnal on võimalik alustada juurpõhjuse ja lahenduse väljatöötamisega. Lahenduse väljatöötamise käigus tekib arusaamine probleemi olemusest ning eesmärgiks on leida probleemile õige ja püsiv lahendus.
* **Tuntud viga** on probleem, mille tekkepõhjus ja ajutine ja/või lõplik lahendus on teada ning need on ka dokumenteeritud. Kui tegemist on tuntud veaga, teeb probleemi omanik probleemihalduse töövahendisse vastavasisulise märke.
* Probleemi lahendaja koos lahendusmeeskonnaga tuvastab probleemi lahendamiseks vajalikud tegevused (sh kommunikatsioon asjaosaliste suunas) ning kirjeldab need probleemipiletis.
* Kui probleemi lahendamise käigus tuvastatakse uus probleem, siis tuleb registreerida uus pilet. Analüüsida tuleb ka infosüsteemi monitooringu osa, ning vajadusel täiendada seiret ning sellest teavitada IT kasutajatuge.
* Kui aktsepteeritakse riski ning ajutine lahendus rahuldab või lõpliku paranduse rakendamine ei ole otstarbekas/puuduvad vahendid, siis kokkuleppel infosüsteemi või infotehnoloogilise vara omanikuga probleem suletakse.

## Probleemi lahendamine ja sulgemine

Lahendus on teadmine viisist, kuidas probleem saab lõplikult ja püsivalt lahendatud. Lahendus realiseeritakse vastavalt probleemi lahendusmeeskonna välja töötatud tegevustele ja tähtaegadele, ning kirjeldatakse kokkuvõtvalt probleemipiletisse. Lahendus paigaldatakse vastavalt muudatusehalduse protsessile ning piletid seotakse (lingitakse).

Probleemi lahendatuks märkimisel tuleb lisada juurde ka kokkuvõte/üldine hinnang. Probleemi sulgemisel märgitakse otsus:

* **Ei ole probleem** - Vajalik ka selgitus hinnangule, et tegemist pole probleemiga.
* **Lahendatud** - Realiseeritud lahendus kõrvaldas algpõhjuse.
* **Tuntud viga** - ajutine lahendus on teada, risk on aktsepteeritud ja probleemi sulgemine lahendust realiseerimata on kooskõlastatud vara omanikuga.
* **Ei lahendata** - risk on aktsepteeritud ning probleemi lahendust ei ole võimalik tuvastada ressursside puudumise tõttu ja/või probleemi lahendamine ei ole majanduslikult otstarbekas, probleemi sulgemine lahendust realiseerimata on kooskõlastatud vara omanikuga.

# Järelevalve

Pöördumiste, intsidentide ja probleemi halduse protsessi järelevalvet teeb regulaarselt kasutajatoe juht, kes pärast pöördumise sulgemist veendub, et pöördumisega seotud asjakohane informatsioon on kogutud, osapooli on teavitatud, vajadusel (intsidentide puhul) järelanalüüs tehtud ja lisatud pöördumise pileti juurde.