pääsynhallintapolitikka

**Luokitus**: Sisäinen

Tätä asiakirjaa ei saa jakaa [Yrityksen] ulkopuolelle ilman omistajan kirjallista lupaa.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Versio | Päivitetty | Muokkaaja | Asiakirjan muutokset | Hyväksyjä | Omistaja |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Sisällysluettelo

[Tämän asiakirjan tarkoitus 3](#_Toc194316963)

[Soveltamisala 3](#_Toc194316964)

[Vastuut 3](#_Toc194316965)

[Pääsynhallinta 3](#_Toc194316966)

[Käyttäjätilien hallinta 3](#_Toc194316967)

[Työsuhteen muutokset tai päättyminen 4](#_Toc194316968)

[Erityisoikeudellisten tilien hallinta 4](#_Toc194316969)

[Käyttöoikeuksien erottelu 4](#_Toc194316970)

[Vähimpien oikeuksien periaate 4](#_Toc194316971)

[Käyttöoikeuksien säännöllinen tarkastaminen 4](#_Toc194316972)

[Käyttäjien salasanahallinta 4](#_Toc194316973)

# Tämän asiakirjan tarkoitus

Tämä asiakirja määrittelee järjestelmien pääsynhallinnan politiikan, tasapainottaen liiketoiminnan ja tietoturvan tarpeet.

# Soveltamisala

Tämä politiikka koskee kaikkia paikallisia ja pilvipohjaisia järjestelmiä. Se on suunnattu esihenkilöille, järjestelmäomistajille, IT-osastolle sekä ylläpitäjille, jotka vastaavat [Yrityksen] datan hallinnasta.

# Vastuut

**Esihenkilöt:**

* Huolehtivat siitä, että työntekijöillä on vain roolinsa kannalta välttämättömät käyttöoikeudet järjestelmiin.
* Hyväksyvät yksilölliset käyttöoikeudet sovelluksiin ja dataan.
* Ilmoittavat välittömästi ja mukauttavat käyttöoikeuksia, kun roolit muuttuvat tai työntekijä poistuu organisaatiosta.
* Tarkistavat säännöllisesti työntekijöiden käyttöoikeustasot.

**Järjestelmäomistajat ja erityisoikeudelliset käyttäjät:**

* Järjestelmäomistaja hallinnoi ja ylläpitää tätä politiikkaa, jos käyttöoikeuksien hallinta ei kuulu IT-osastolle.

**IT-tuki:**

* Myöntää käyttöoikeuksia järjestelmiin ja tarkistaa käyttöoikeuspoikkeamat.

# Pääsynhallinta

## Käyttäjätilien hallinta

* Jokaisella käyttäjällä on yksi henkilökohtainen ei-admin -tason käyttäjätili per järjestelmä. Poikkeukset vaativat hyväksynnän esihenkilöiltä.
* Käyttäjätunnukset ovat henkilökohtaisia ja yksilöllisiä.
* Prosessit käyttäjien lisäämiseen, muokkaamiseen ja poistamiseen on määriteltävä selkeästi.
* Käyttöoikeudet järjestelmiin voidaan myöntää vain esihenkilön tai järjestelmäomistajan hyväksynnällä.
* Käyttöoikeudet on päivitettävä liiketoiminnan muutosten, roolimuutosten ja käyttäjän organisaatiosta poistumisen yhteydessä.
* Kaikki käyttöoikeusmuutokset on dokumentoitava.
* Vain koulutetut työntekijät saavat hallinnoida käyttäjätunnuksia.
* Kullekin järjestelmälle on määriteltävä käyttöoikeuskäytännöt siten, että ne eivät haittaa työntekoa.
* Käytä monivaiheista tai kaksivaiheista tunnistautumista (MFA, 2FA) lisäturvaa varten.
* Hyödynnä kertakirjautumista (Single-Sign-On/SSO) keskitetyn käyttöoikeushallinnan mahdollistamiseksi.

## Työsuhteen muutokset tai päättyminen

* Ilmoita HR:lle, IT:lle ja muille osastoille roolimuutoksista tai työntekijän lähtemisestä.
* Ulkoisten osapuolten sopimusmuutoksista on tiedotettava järjestelmän käyttöoikeuksien hallinnoijalle.

## Erityisoikeudellisten tilien hallinta

* Kaikki erityisoikeudellisten tilien muutokset on dokumentoitava.
* Vältä geneerisiä admin-tilejä (*admin, root, sa, dba, administrator, jne*) auditoinnin mahdollistamiseksi.
* Kaikkien admin- ja erityisoikeudellisten tilien on perustuttava niiden työnkuviin.

## Käyttöoikeuksien erottelu

* Ylläpitäjien on käytettävä erillisiä yleisiä ja erityisoikeudellisia tilejä.

## Vähimpien oikeuksien periaate

* Käyttäjille myönnetään vain heidän roolinsa kannalta välttämättömät käyttöoikeudet.

## Käyttöoikeuksien säännöllinen tarkastaminen

* Tarkasta tilit [tarkastustiheys] ja poista käyttämättömät.

## Käyttäjien salasanahallinta

* Varmista, että kaikissa [Yrityksen] järjestelmissä on käyttäjätunnus ja salasana, jotka noudattavat [Yrityksen] salasanapolitiikkaa.