**AD Admin Groups Governance Process**

Date: 20/04/2018

Description: E:\Duunit\SEK - metsaliitto\WMF\Metsa_logo_vaaka_RGB.wmf

Track: Active Directory & Printer Management

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Prepared by / Modified by | Significant Changes |
| 1.0 | 11/04/2018 | Sugandh Gandham | Draft |
| 1.1 | 20/04/2018 | Sugandh Gandham | Significant Changes |

Table of Contents:

1. [Introduction………………………………………………………………………………..3](#_Introduction:)
2. [Purpose……………………………………………………………………………………...3](#_Purpose:)
3. [Scope………………………………………………………………………………………….3](#_Scope:)
4. [AD Admin Groups Information…………………………………………………...3](#_Admin_Groups_Information:)
5. [Current Process…………………………………………………………………………..4](#_Current_Process:)
6. [New Process……………………………………………………………………………….4](#_New_Process:)

# Introduction:

This document is to define the process of handling Administrative Rights for AD Admin Groups.

The intended audience for this document is:

* HCL AD & Printer Management Team
* Metsa

# Purpose:

The purpose of the process is to:

* Define the Governance process of handling any Administrator Rights delegation in Active Directory
* Define communication process for requesting admin access among HCL, Metsa and other vendors

# Scope:

Below is the scope of the process:

* Domain Admins
* Schema Admins
* Enterprise Admins Rights delegation

# AD Admin Groups Information:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **AD Admin Groups** | **HCL** | **Metsa** | **Tieto** | **Other Vendors** |
| Domain Admins | 12 | 8 | 31 | 17 |
| Schema Admins | 0 | 1 | 0 | 0 |
| Enterprise Admins | 2 | 4 | 19 | 3 |

# Current Process:

Whenever a user has been added or removed from Domain Admins, Schema Admins and Enterprise Admins an email alert will be generated to AD Team. HCL AD Team will inform Service Owner about this and based on their inputs HCL AD Team will take necessary actions.

**5.1) HCL:**

AD team receives a request from respective Reporting Manager with business justification. Based on request, HCL will seek approval from Metsa Service Owner. AD team creates a Service Request and provides needed access for the requested accounts.

**5.2) Tieto:**

Tieto has a tool which adds users to admin groups and apart from that Tieto admins also delegate Domain Admins, Enterprise Admins rights to users. Modifications to AD admin groups are being done even without Serve-me tickets.

**5.3) Metsa/Other Vendors:**

HCL AD Team might or might not receive request to delegate Administrator Rights for users as modifications to AD admin groups are being done even without Serve-me tickets.

# New Process:

We would like to propose the below process for robust governance and control over AD admin groups to prevent any unauthorized access.

1. User will request for adding/deleting any member to/from AD admin groups with a Business Justification, RM approval and time duration to HCL AD Team.
2. HCL AD Team will open a Service Request for the requested task.
3. HCL AD Team evaluates the request and validates the business justification. In case, the HCL AD Team finds that the Administrator Rights requested; are not needed for the provided Business Justification then the Team will suggest the desired access level to the requestor.
4. In case of limited duration, HCL AD Team will delegate the Administrator Rights to the requested account. However, in cases where permanent access is being requested, HCL AD Team will evaluate the reason and risk in granting the Administrator Rights and convey its inputs to the requestor. Example: Requestor wants to manage DNS records and has requested Domain Admins rights. So we will suggest that we can add/remove users to the DNS Admins group to mitigate the risk.
5. Once agreed with requestor on the desired access level and time duration, HCL AD team will seek approval from the Service Owner, upon approval delegate the needed access to the requested account and close the Service Request.