Active Directory and Email Access Management

Policy Statement

This policy is meant to control the handling of user accounts and it ensures that the users and their pertaining equipment are registered on the domain through a proper channel. This policy ensures that the access of the users to the information assets and email services is managed according to their job function.

Objective

The purpose of this Policy is to minimize risk associated with Active Directory and E-mail services and defines controls against the threats of unauthorized access and theft of information/services.

Prerequisite

This Policy should be read in conjunction with:

- Information Security Policies, including
- Access Control Policy

Responsibility

- Email Server and Active Directory Administrator
- Unit Head/Team Lead
- Head of Department (Business Head)
- User
- HR

Procedure

Step	Description	Responsibility
Email Access		
1.	The HR Department registers the new joiner in HR Management System. Relevant Head of Department/team lead, or respective senior of the joiner shall lodge a request for the email-id and network id of new joiner in the SFR/RMS Portal and the request is forwarded to the System Administrator in the IT Department which will grant AD Identity and email ID for the new joiner as per the request.	HR/ Relevant Head of Department/Relevant Team Lead/ IT Department
2.	If an AD/ network and email id for existing employee is required, the user shall generate a request in the RMS Portal, which will be approved by Head of Department. After necessary approval from the Head, the request is forwarded to IT Department for action.	User/ Head of Department (Business Head)/Team Lead (Business Department)
3.	The RMS request for the generation of new network and email ID shall be checked for relevant approval.	System Administrator
4.	AD and Email ID shall be created using information specified in the SFR / RMS request. (First Name, Last Name, Department, Title, Employee ID) by the relevant administrator.	System Administrator
5.	User will be assigned a unique Domain ID and email ID and his/her computer shall be configured with domain and email access and as per the given department information user should be added in respective departments email groups.	System Administrator
Operational & Monitoring		
1.	Appropriate restrictions shall be placed e.g. block sending of exe files, set email attachment limits, installation restrictions, sensitive windows file access restrictions etc.	System Administrator
2.	Email disclaimer, as stated in Access Control Policy, must be added underneath the signature by the server.	System Administrator
3.	Content scanning may be done to detect fraud emails. If found they shall be reported to the Group Head Digital, Technology and Strategic Planning.	System Administrator
Terminated Employees / Leavers		
1.	IT Department shall be informed of Terminated Employee/Leaver. And as soon the employee is end dated in HR Management System by HR a . User deletion process request should be initiated through HR.	HR
2.	Backup of all emails and important files to be taken of Terminated Employee/Leaver and data can be retained as per business requirements.	User