# Account and Password Policy

# Hex Secure Framework

VERSION: 1.2 REVISION DATE: Apr 19, 2025

# Contents

# Section 1 Purpose

The purpose of this document is to define a secure account and password policy for Hexagon Group. This policy is critical for safeguarding user access, protecting sensitive information, and ensuring system integrity. By enforcing strong authentication practices, structured account management, and regular password controls, Hexagon Group enhances its cybersecurity posture, reduces the risk of unauthorized access, and supports the continuity of secure business operations.

# Section 2 Account Policy

## 2.1 Account Naming Policy

- All accounts must follow a consistent naming convention (e.g., firstname.lastname).
- Service accounts must reflect their role and system (e.g., svc.backup01).

## 2.2 User and Group Policy

- Users are assigned roles via security groups with least privilege access.
- Groups are reviewed quarterly for accuracy.

## 2.3 Admin Account Policy

- Admin accounts are strictly controlled and separated from user accounts.
- All activities are logged.

## 2.4 Guest and Vendor Account Policy

- Temporary accounts for guests/vendors must have expiration dates.
- Access must be monitored and limited to required resources.

# Section 3 Password Policy

## 3.1 User Password Requirements

- Minimum 12 characters; include upper/lowercase, number, symbol.
- Passwords expire every 90 days; last 5 cannot be reused.

## 3.2 Admin Password Requirements

- Stronger complexity enforced; rotation every 60 days.
- Multi-Factor Authentication (MFA) is mandatory.

## 3.3 LAPS (Local Admin Password Solution)

- Local admin passwords are randomized and securely stored.
- Only authorized personnel may retrieve credentials.

## 3.4 Wi-Fi Password Policy

- Different SSIDs for staff, guests, and IoT.
- Guest passwords rotate weekly; staff use secure domain login.

# Section 4 Implementation and Review

## 4.1 Account Provisioning

- Created only with manager and HR approval.
- Access rights assigned based on job role.

## 4.2 Deactivation and Deletion

- Deactivated immediately after employment ends.
- Final deletion after 30 days of inactivity.

## 4.3 Policy Audits

- Quarterly audits for compliance.
- Adjustments made based on audit findings and security incidents.

## 4.4 User Training

- Users must attend annual security training.
- Includes secure password handling and phishing awareness.

# Section 10 References

| Document No. | Document Title | Date | Author |
|---|---|---|---|
| | | | |
| | | | |