==

CATEGORY: WindowsSecurityPolicies (Local Security Policy / SecEdit)

==

Local Security Policy operations directly affect authentication, authorization, audit controls, password policy, privilege assignments, and system hardening. These SOPs ensure every security-policy action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with enterprise security and compliance standards.

SOP 1 – Export Local Security Policy

1. Purpose

Export the current Local Security Policy to an INF file for backup, audit, or replication.

2. Scope

- **Windows servers and workstations**
- **Local Security Policy (secpol.msc)**

3. Preconditions

- **Operator must have administrative rights**
- **Export path must be valid**

4. Required Inputs

- **Export file path**

5. Procedure Steps

- **Input Collection**
- **Export Operation** – Use SecEdit to export policy.
- **Post-Export Verification**

- **Logging**

6. Expected Output

- **Security policy exported successfully**

7. Error Handling

- **Access denied**
- **Invalid path**

8. Security Considerations

- **Exported policy files may contain sensitive configuration**

9. Audit Logging Requirements

- **Operator ID**
- **Export path**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures security configurations can be backed up or replicated consistently, supporting compliance and disaster recovery.

SOP 2 – Import Local Security Policy

1. Purpose

Apply a Local Security Policy from an INF file.

2. Scope

- **Windows servers and workstations**

3. Preconditions

- **Operator must have administrative rights**
- **Import file must exist**

4. Required Inputs

- **Import file path**

5. Procedure Steps

- **Input Collection**
- **File Validation**
- **Import Operation –** Apply policy using SecEdit.
- **Post-Import Verification**
- **Logging**

6. Expected Output

- **Security policy applied successfully**

7. Error Handling

- **Invalid INF file**
- **Access denied**

8. Security Considerations

- **Imported policies may override critical security settings**

9. Audit Logging Requirements

- **Operator ID**
- **Import path**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures security policies are deployed consistently and safely, supporting compliance and system hardening.

SOP 3 – Get Password Policy Settings

1. Purpose

Retrieve password-related security settings from Local Security Policy.

2. Scope

- **Windows servers and workstations**
- **Local Security Policy → Account Policies → Password Policy**

3. Preconditions

- **Operator must have permission to query security settings**

4. Required Inputs

- **None**

5. Procedure Steps

- **Policy Query –** Retrieve password policy values.
- **Attribute Extraction –** Length, complexity, history, max/min age.
- **Output Formatting**
- **Logging**

6. Expected Output

- **Password policy details**

7. Error Handling

- **Access denied**
- **Policy retrieval failure**

8. Security Considerations

- **Password policy is a core security control**

9. Audit Logging Requirements

- **Operator ID**
- **Timestamp**

10. Organizational Benefit Statement

This procedure provides visibility into password requirements, supporting compliance and identity-security enforcement.

SOP 4 – Get Account Lockout Policy

1. Purpose

Retrieve account lockout thresholds and durations.

2. Scope

- **Windows servers and workstations**
- **Local Security Policy → Account Policies → Account Lockout Policy**

3. Preconditions

- **Operator must have permission to query security settings**

4. Required Inputs

- **None**

5. Procedure Steps

- **Policy Query**
- **Attribute Extraction –** Lockout threshold, duration, reset time.
- **Output Formatting**
- **Logging**

6. Expected Output

- **Account lockout policy details**

7. Error Handling

- **Access denied**

8. Security Considerations

- **Weak lockout settings increase brute-force risk**

9. Audit Logging Requirements

- **Operator ID**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures administrators can verify lockout protections, supporting identity security and compliance.

SOP 5 – Get User Rights Assignment

1. Purpose

Retrieve privilege assignments (e.g., log on locally, shut down system).

2. Scope

- **Windows servers and workstations**
- **Local Security Policy → User Rights Assignment**

3. Preconditions

- **Operator must have permission to query security settings**

4. Required Inputs

- **Optional: Specific privilege name**

5. Procedure Steps

- **Input Collection**
- **Policy Query**
- **Privilege Extraction –** Users/groups assigned to each right.
- **Output Formatting**
- **Logging**

6. Expected Output

- **Privilege assignment details**

7. Error Handling

- **Privilege not found**
- **Access denied**

8. Security Considerations

- **Privilege assignments directly affect system security**

9. Audit Logging Requirements

- **Operator ID**
- **Privilege name (if provided)**

- **Timestamp**

10. Organizational Benefit Statement

This procedure provides visibility into privilege assignments, supporting security audits and least-privilege enforcement.

SOP 6 – Apply Security Template

1. Purpose

Apply a predefined security template (INF) to enforce hardening standards.

2. Scope

- **Windows servers and workstations**
- **Security templates (CIS, STIG, custom)**

3. Preconditions

- **Operator must have administrative rights**
- **Template must be approved by security**

4. Required Inputs

- **Template file path**

5. Procedure Steps

- **Input Collection**
- **Template Validation**
- **Apply Template –** Use SecEdit to enforce settings.
- **Post-Apply Verification**
- **Logging**

6. Expected Output

- **Security template applied successfully**

7. Error Handling

- **Invalid template**
- **Access denied**

8. Security Considerations

- **Templates may override critical system settings**

9. Audit Logging Requirements

- **Operator ID**
- **Template path**
- **Timestamp**

10. Organizational Benefit Statement

This procedure ensures consistent, policy-driven hardening across systems, supporting compliance and reducing attack surface.