# Security Incident Management Workflow – Credential Compromise

**Detection** | **Analysis** | **Containment** | **Eradication** | **Recovery** | **Post-Incident Activities**

**End User**

START

End-user detection

**Help Desk**

Open help desk ticket

Help desk analysis

Credential compromise?

NO

YES

Tier 3

YES

Tier 2

YES

Tier 1

YES

Reissue devices, if applicable

**Cybersecurity**

START

Cybersecurity detection

Open incident record

Cybersecurity analysis

False positive?

NO

YES

Tier 2 Tier 1 Tier 1

Run vulnerability & anti-malware scans

Conduct post-incident analysis

Update/close incident ticket

**IT Operations**

Validate any suspicious login events

Disable compromised credentials

Remote-wipe missing devices

Reset potentially compromised accounts

Restore any affected systems/data

**CISO**

CISO analysis

Inform sr. mgmt.?

NO

YES

**Legal, PR, HR**

Legal, HR, PR analysis

**Sr. Mgmt.**

Senior management analysis

Facilitate post-incident lessons-learned meeting

**External**

Tier 3
Report a crime to law enforcement

END