Network Breach Containment Checklist

Immediate Containment Steps

- [ ] Isolate affected systems from the network
- [ ] Disable compromised user accounts and credentials
- [ ] Block malicious network traffic at firewall
- [ ] Preserve evidence and maintain logs
- [ ] Remove unauthorized physical devices (if any)

Notification

- [ ] Notify IT security team and management
- [ ] Inform legal or compliance if required
- [ ] Communicate with third parties as per policy

Containment Validation

- [ ] Confirm threat has been contained
- [ ] Monitor network for further suspicious activity
- [ ] Document containment measures applied

Notes

Additional information / Observations: