Security Posture Assessment Worksheet

BLACKHAWK DATA

Identity & Access

- □ MFA enabled for all users
- □ SSO deployed for cloud applications
- □ Privileged access management in place
- □ Password policy meets industry standards
- □ Regular access reviews conducted

Network Security

- □ Network segmentation implemented
- □ East-west traffic inspection enabled
- □ Wireless security (WPA3/802.1X)
- □ Guest network isolated
- □ IoT/OT devices segmented

Endpoint Security

- □ EDR deployed on all endpoints
- □ Patch management process in place
- □ Device encryption enforced
- □ USB device controls enabled
- □ Mobile device management deployed

Email & Web Security

- □ Email gateway with anti-phishing
- □ DMARC/DKIM/SPF configured
- □ Secure web gateway deployed
- □ URL filtering enabled
- □ Attachment sandboxing active

Monitoring & Response

- □ SIEM deployed and monitored
- □ Incident response plan documented
- □ Incident response tested in last 12 months
- □ Vulnerability scanning scheduled
- □ Penetration testing conducted annually

Compliance

- □ Compliance framework identified (NIST, CIS, HIPAA, PCI, NERC CIP)
- □ Last compliance audit date
- □ Data classification policy exists
- □ Security awareness training conducted
- □ Third-party risk assessment process