CompTIA IT Security COMMUNITY

THE FUNDAMENTAL BL21KS

CRITICAL

ACCEPTABLE USE POLICY
Written policy defines enforcement.

NEXT GEN FIREWALLS
Leverage advanced and extensible security platforms.

ADVANCED ENDPOINT DEFENSE
Use next gen advanced endpoint defense.

PROTECTIVE FILTERING
Scrub email in the cloud, enable click protect and filter controls at the edge.

PATCH APPROVAL & MANAGEMENT
Keep systems reliably patched and up-to-date.

BACKUPS
Offsite, encrypted, and regularly tested.

PASSWORD POLICY
Use strong passwords and follow best practices.

USER AWARENESS TRAINING
Empower people to spot a threat and reduce risk.

TWO FACTOR AUTHENTICATION
Use anywhere compatible.

NETWORK ASSESSMENT
Use assessments to identify risks.

DNS
Leverage secure DNS providers.

DARKWEB SEARCH
Monitor the dark web for compromised credentials and sensitive data.

CRITICAL+

THREAT HUNTING
Deploy advanced detection tools to identify threats.

INTERNET OF THINGS
Segment, segment, segment, plus access control.

COMPLIANCE

ACCESS CONTROL
Role & permission based access.

SIEM
Complete visibility + compliance reporting.

CHANGE MANAGEMENT
Maintain accountability of who did what, when.

DATA ENCRYPTION
Protect in motion and at rest.

DIGITAL CERTIFICATES
Verify identity and encrypt data in transit.

ENCRYPTED CONFIG BACKUPS
Automate and encrypt device backups.

BUSINESS CONTINUITY / DISASTER RECOVERY PLAN
Keep the business running!