RIVIAL Data Security

IT AUDIT CHECKLIST

Application Access Controls

□ User accounts provisioned

□ Access levels modifiable, user privileges limited to job function

□ Periodical access reviews scheduled

□ Password complexity requirement

□ Admin activity monitored

Database Access Controls

□ Database admin accounts controlled

□ Admin activity monitored

□ Application access to database restricted

Operating System Access Controls

□ System installation checklists or images used

□ Security and event logs enabled

□ Unnecessary services turned off

Virtual Access Controls

□ Access to hypervisors restricted

□ Access levels modifiable

□ Periodical access reviews

□ Password complexity requirement

□ Secure configuration guide applied to hypervisors and SANs

□ Access to services running on host restricted

Network Access Controls

□ Firewall for remote access

□ IDS for remote access

□ IPS for remote access

□ VPN for remote access

□ MFA for remote access

Physical Security Controls

□ Physical perimeter protections

  □ Locks

  □ Badge access

  □ Battery backup up

  □ Generators

  □ HVAC

Anti Malware Controls

□ Anti-virus software

□ Gateway filtering

□ Browser protections

Vulnerability Management Controls

□ Scanning and remediation for vulnerabilities

□ Patch management program

IT AUDIT CHECKLIST

Software Development Controls

□ Software development lifecycle established
□ Secure coding and web app firewall/security testing

Change Management Controls

□ Process for change management instated
□ Inventory of IT assets

Disaster Recovery Controls

□ Backups for systems and data
□ Disaster recovery plan established and regularly tested
□ Business impact analysis plan established and regularly tested

Vendor Management Controls

□ Security clauses included in contracts
□ SLA's are monitored
□ Vendor incident notifications sent to subservice organizations

Incident Management Controls

□ Incident response plan instated and regularly tested
□ Customers notified following vendor incidents

User Awareness Controls

□ Users trained on security
□ Background checks for new employees
□ Duties separated and documented
□ Security logs collected and reviewed

Data Protection Controls

□ Encryption in transit and at rest
□ Data classification
□ Usb restrictions in place
□ Removal of data from storage media

Asset Management Controls

□ Hardware and software inventoried
□ Installation of unauthorized software, utility and audit tools prohibited
□ System capacity and performance monitored

Security Program Controls

□ Risk assessments regularly performed regularly
□ Risks mitigated to acceptable levels
□ Information security policies approved and in place
□ Periodical independent audits performed