DATABANK
Data Center Evolved™

FedRAMP COMPLIANCE CHECKLIST

PHYSICAL ACCESS CONTROLS

Physical Security (Data Center Access)

- Restricted Access to the Facility
- Signs for Identifying the Data Center
- Guard or Attendant at Entrance
- Photo ID Required
- Sign-in/Sign-out Process
- Two Factor Authentication

Data Center Security and Facility: Access rights

- Restricted Access to DC Facility
- Two-Factor Access Required
- Signs Posted for Restricted Access
- Unique Access ID for Each Employee/person
- Process For Granting/ Revoking Access
- Escort Required for Visitors/Vendors
- Regularly Recurring Access Review

Data Center Security and Facility: Access tracking

- Live Monitoring of Accesses
- Digital Log of Door Accesses
- Visitor Log
- Camera Placement at All Door Access Points, Aisles/Cages

Data Center Security and Facility: Data protection

- Shredder Present
- Server/Comm Cabinets Secured
- Network Cables and Sockets Secured

LOGICAL ACCESS CONTROLS

Data Center Security and Facility: Data Protection (continued)

- Complete Separation Between Each Customer Environment (CoLo)
- Separate & Defined Server Roles
- Access Control and Logging for All Access to Servers with PHI
- Firewall Between Public/ Private Zones
- Production Change Management
- Incident/Problem Management Program
- Security Incident Response Plan
- Risk Management

Documented Policies/Controls

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Physical and Environmental
- Planning
- Program Management
- Personnel Security
- Risk Assessment
- Systems and Services Acquisition
- Systems and Communications
- Systems and Info Integrity

NETWORK ACCESS CONTROLS

Firewall

- Dedicated HA Firewall for Every Environment
- Complete Logical Isolation for Customers
- Point-to-Point IPSEC VPN Tunnels
- Multi-Factor Authentication
- FIPS140-2 Encryption
- INGRESS and EGRESS Filters
- Access Control List Managements

Network

- Private VLAN
- DMZ Zone for Public Services
- Internal Zone for Private Server
- All Customers Must Have HA Pair Firewalls

Intrusion Prevention

- IIntrusion Detection Service
- Intrusion Prevention Service
- Prevention of “Phone Home Bots”
- DDoS Mitigation
- Web Application Firewalls for OWASP 10
- Management of IDS Rules & Blacklist Maintenance of WAF Rules

Enterprise: Anti-virus

- Enterprise-Grade Anti-Virus
- Host-Based Intrusion Prevention
- Centralized Reporting
- Abnormal Process Logging

MANAGED HOSTING

Business Checklist

- Utilize Data Encryption
- Appropriate Insurance Coverage
- Onsite and Offsite Backups
- Vulnerability Management and Logging
- Have Adequate Security, Incident, Training and HR Policies
- SSAE 18 SOC 2 Type II
- Participate in Your Audit(s) at Extra Cost
- Specific Compliance Training
- Security Awareness Training

Managed Hosting Checklist

- Comprehensive Monitoring
- Performance Dashboards Responsible for Responding to Alarms, Restoring Service and Escalations 24/7/365
- Secure Ticketing Portal
- Dedicated Technical Account Manager
- Dedicated Implementation Engineer
- 24/7/365 Phone/Ticket Tech Support
- Patching
- File Integrity Monitoring
- Log Offloading
- Hardened OS Images
- SSP - 40 hours at $200 per hour