

# AppExchange Certification Requirements Checklist

## Policies

- Security (Master Policy)
- Data Handling
- Acceptable Use
- Encryption
- Network/System Configuration
- Patch Management
- Software Development
- Change Control
- System Access
- Application Security
- Data Privacy
- Log Management
- Personnel Security
- Physical Security
- Incident Management
- Business Continuity
- Disaster Recovery

## Standards & Procedures

- System Configuration
- Application Development
- Application Configuration
- Database Configuration
- Network Configuration (Including Firewall/IDS)
- Patching Process
- User Provisioning/De-Provisioning
- Logging Process/Log Review
- Pre-employment Security Review
- Physical Security
- Incident Management Process
- Authentication & Authorization
- Encryption Standard

## Network Security Implementation

- Stateful Packet Inspection Firewall with NAT implemented
- Web/Application servers on a DMZ separated by a second firewall layer (logical or physical) from the database server
- Network IDS/IPS implemented
- Log Management implemented
  - Log retention for at least 1 year
  - Log aggregation and alerting for all network devices and systems
  - Log aggregation for application logging
  - Log aggregation for database logging (optional)
- Wireless Networking
  - No wireless in collocation facilities
  - WPA2 and wireless IDS implemented at corporate (required if VPN connection exists between corporate and collocation facility)
- E-mail Spam filter and Anti-virus (required if e-mail is used by your product)

## Optional Network Security Add-ons

- Application Firewall
- Network Database Logging/IDS solution
- Automated Log Correlation across the network

## Host/Platform Security Implementation

- Implement a System Configuration Standard
  - Remove unnecessary services
  - Harden services as required
  - Remove/Rename default accounts and change passwords
  - Encrypt all passwords
  - Unique usernames
  - Implement a robust password policy
    - Minimum 8 characters
    - Combination (3 out of 4) of numbers, letters (lower and upper) and special characters
    - Enable lock outs for bad attempts (3-5)
    - Enable password expiration (90 days)
    - Enable password history (don't allow reuse of last 8 passwords)
  - Implement system logging/aggregation as noted above in Network section
  - Implement host based firewalls
- Implement Secure Remote access (VPN – SSHv2, SSL, IPSEC 3DES, or AES)
  - Persistent tunnels configured with appropriate ACLs
- Implement robust patch management
- Implement comprehensive anti-virus

## Optional Host/Platform Security add-ons

- Implement Host IDS solution
- Implement Configuration Management Tool
- Implement Encrypted file systems or databases could
- Implement an enterprise password vault

## Application Development Security Implementation

- Implement an Application Development Standard
  - Implement Software Development Policy
  - Implement Change Management Policy
  - Implement Code Reviews
  - Implement a Testing/QA Methodology
  - Implement a Methodology for Rolling Code to Production
  - Implement Appropriate Segregation of Duties
- Unless Necessary, Do Not Store Salesforce.com Credentials
  - If Necessary, Have a Clear Rationale
  - Communicate to Salesforce.com Your Rationale
  - Implement a Process for Updating the Password
- Implement Encryption
  - SSLv3
  - Do Not Store Encryption Keys in Source Code
  - Implement Encryption Key Management
- Avoid Dynamic SQL
  - If Using Dynamic SQL, Prepare Appropriate Rationale for Salesforce.com
  - Implement Appropriate Compensating Controls

- Implement Appropriate Input Validation
- Implement Authentication & Authorization Standard
- Implement Pre-Production Testing Methodology
  - Implement Anti-virus check prior to packaging software for production

### Optional Application Development Security add-ons

- Implement Source Code Checking Tools
- Implement SQL Checking Tools
- Implement Application Firewalls
- Implement Database IDS/Logging Solution

### Operational Security Implementation

- Align Operational Behavior with Written Policies, Standards, and Procedures
- Actively Monitor Your Network
  - Monitor Your Log Aggregation/Correlation Solution
  - Implement Network and System Monitoring Solution
  - Implement an Incident Management Process
- Implement Disaster Recovery and Business Continuity Plans
- Implement an Employee Training Program
  - One Hour Minimum Each Year for All Employees
  - Security Personnel Training At Least 40 Hours Each Year
- Implement Encryption Key and Privileged User Password Rotation

### Operational Security add-ons

- ISO 27001 Implementation and Certification
- SAS70 Certification
- Other Certifications Relevant to Industries Your Company Supports