### 4: Access Control (cont.)

| 4.1.11 | Sessions idle for more than 15 minutes should require users to re-authenticate (e.g. Screen Lock) |
| 4.1.12 | Users should not be allowed local admin privileges |
| 4.1.13 | Vendor access should be approved and monitored |
| 4.1.14 | Administrative account passwords (e.g. root or enterprise domain admin account) should be managed centrally in a secure repository |
| 4.1.15 | Default passwords should be changed in applications and devices |
| 4.1.16 | Access to administrative interfaces on devices should be denied from the Internet |

### 5: Physical Security

| 5.1.1 | An inventory of publically accessible network jacks should be maintained |
| 5.1.2 | Access to publicly accessible network jacks should be restricted |
| 5.1.3 | System backups should be stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility |
| 5.1.4 | Servers should be kept in a locked room |

### 6: Monitor Access to Info Systems

| 6.1.1 | Critical system clocks should be time synchronized through the use of time synchronization technology |
| 6.1.2 | Viewing of log files should be limited to those with a job-related need |
| 6.1.3 | Log files should be promptly backed up to a centralized log server |
| 6.1.4 | Follow-ups to exceptions in log files should be required |

### 7: Info Security Policy Awareness (cont.)

| 7.2.1 | The IReport Policy should be adhered to at all times |
| 7.3.1 | The Electronic Devices policy should be adhered to at all times |
| 7.4.1 | The IDispose Policy should be adhered to at all times |
| 7.5.1 | The Responsible Use of Information Technology Policy should be adhered to at all times |

### 8: Supporting Process

| 8.1.1 | An inventory process for tracking additions and removal of IT assets including servers, workstations, printers, firewalls, and other network devices should be documented and followed |
| 8.1.2 | An inventory process for tracking custom applications, purchased software, and databases should be documented and followed |
| 8.1.3 | A documented change management process for tracking changes to firewalls, servers, workstations, printers, and other network devices should be followed |
| 8.1.4 | Documented patch management processes and procedures for servers and workstations should be followed |
| 8.1.5 | Documented patch management processes and procedures for custom applications and purchased software should be followed |
| 8.1.6 | Documented processes and procedures for the storage and disposal backup media should be followed |
| 8.1.7 | Documented processes and procedures for auditing all system and user account roles and access should be followed |
| 8.1.8 | A continuity of operations plan should be documented and maintained |
### 1: Network Security

- 1.1.1 Protect networked devices with a firewall(s)
- 1.1.2 Firewall operators should complete the DoIT firewall training class
- 1.1.3 Firewalls should restrict inbound connections to systems of interest
- 1.1.4 Firewalls should send logs to the OCIS security event manager
- 1.1.5 Firewall rule changes should be documented and tracked
- 1.1.6 Firewall rules should be reviewed annually
- 1.2.1 External vulnerability scans should be performed semi-annually
- 1.2.2 Appropriate personnel should review the results
- 1.2.3 Vulnerabilities should be remediated within 30 days
- 1.2.4 Internal vulnerability scans should be performed semi-annually
- 1.3.1 An inventory of workstations should be maintained at all times
- 1.3.2 Appropriate personnel should review the results
- 1.3.3 Vulnerabilities should be remediated within 30 days
- 1.4.1 Alerts from OCIS should be monitored and responded to
- 1.5.1 Departmental wireless access points should be managed

### 2: Maintain Secure Endpoints

#### 2.4 Maintain an inventory of applications installed on servers at all times

- 2.4.1 Install managed antivirus software on all workstations and servers (Example Symantec Endpoint Protection)
- 2.4.2 Antivirus programs should report to a central console
- 2.4.3 Antivirus programs should be configured to check for new signatures every 24 hours
- 2.4.4 Clients should be set to scan endpoints at least weekly

#### 2.5 Patch third party applications within 30 days of release

- 2.5.1 Install Identity Finder on all endpoints
- 2.5.2 Identity Finder should be configured to scan user directories
- 2.5.3 Identity Finder should be configured to scan for formatted restricted data
- 2.5.4 Identity Finder should be configured to check for updates weekly
- 2.5.5 Identity Finder scan results should report centrally
- 2.5.6 Identity Finder should be configured to scan every 30 days

#### 2.6 Remove end-of-life applications from endpoints

- 2.6.1 The Center for Internet Security templates should be used as a baseline for creating common operating system configurations for workstations and servers
- 2.6.2 Unnecessary services should be disabled prior to servers moving to production
- 2.6.3 Open relay services should be disabled on email servers

#### 2.7 Maintain an inventory of applications installed on workstations at all times

- 2.7.1 Secunia: Corporate Software Inspector should be installed on all supported workstations
- 2.7.2 Maintain an inventory of applications installed on workstations at all times
- 2.7.3 Secunia: Corporate Software Inspector should be installed on all supported workstations

### 3: Application Development Security

- 3.1.1 Maintain a central inventory of custom applications
- 3.1.2 Maintain a central inventory of all database services
- 3.1.3 Web logs, access logs, and security logs should be reporting to the OCIS security event manager
- 3.1.4 Source code should be stored in a source code repository
- 3.1.5 SSL encryption should be required for sensitive pages
- 3.1.6 Certificates should be valid, not expired, not revoked, and match all domains used by the site
- 3.1.7 Maintain an inventory of active certificates
- 3.1.8 IBM AppScan should be run using the OWASP Top 10 as a template on all custom web applications and web sites
- 3.1.9 All databases should be scanned using the McAfee Vulnerability Manager for Databases

### 4: Access Control

- 4.1.1 All users should be assigned a unique ID before allowing them to access system components or restricted Data
- 4.1.2 System administrations should not use admin accounts for general purpose computing
- 4.1.3 Users identities should be verified before performing password resets
- 4.1.4 First-time and reset passwords should be set to a unique value for each user
- 4.1.5 Each user should be required to change their password immediately after the first use
- 4.1.6 Processes should be in place for deactivating user accounts under emergency circumstances such as terminations, compromise, or infection
- 4.1.7 Inactive user accounts over 90 days old should either be removed or disabled
- 4.1.8 Passwords should adhere to the University of Wisconsin - Madison Chief Information Officer's official password policy
- 4.1.9 Service accounts should be used for internal application and database operations
- 4.1.10 Repeated access attempts should be limited by locking out the user ID after no more than six attempts for at least 15 minutes