## Minimum Security Standard: Applications

<table>
<thead>
<tr>
<th>Standard</th>
<th>What to do</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patching</td>
<td>Systems that store, process, or access <strong>Sensitive</strong> data should be patched within two weeks of a security update addressing a <strong>Critical</strong> or <strong>High vulnerability</strong> becoming available. Systems that store, process, or access <strong>Restricted</strong> or <strong>Public</strong> data should be patched within four weeks of a security update addressing a <strong>Critical</strong> or <strong>High vulnerability</strong> becoming available.</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>ITSO conducts monthly scans, which may uncover vulnerabilities on hosts or applications. Departments should use Security Center to identify and remediate vulnerabilities. Remediate <strong>Critical</strong> and <strong>High vulnerabilities</strong> within 14 days. Do not explicitly block our vulnerability scanning.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Permit the minimum necessary services through any departmental network firewalls and/or host-based protections.</td>
</tr>
<tr>
<td>Credentials and Access Control</td>
<td>Review existing accounts and privileges annually. Enforce password complexity. Web application logins with credentials via SAML required.</td>
</tr>
<tr>
<td>Two-Step Authentication</td>
<td>Require multi-factor authentication[^4] for all administrator logins (PRS) and interactive users of RS applications.</td>
</tr>
<tr>
<td>Centralized Logging</td>
<td>Forward logs to a remote log server. University IT Splunk service recommended.</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure Software Development</td>
<td>Include security as a design requirement. Review all code and correct identified security flaws prior to deployment. Use of static code analysis tools recommended.</td>
</tr>
<tr>
<td>Monitor for Application Security Updates</td>
<td>Join and monitor security and development lists to receive notification of updates.</td>
</tr>
<tr>
<td>Backups</td>
<td>Regular backup and encryption [5] is recommended. Note that not all Sensitive or Restricted application data is permitted to be backed up.</td>
</tr>
<tr>
<td>Administrative Account Access</td>
<td>Use separate administrative and personal accounts. Manage group passwords with a password manager.</td>
</tr>
<tr>
<td>Security Review</td>
<td>Request a Vendor Risk Assessment prior to signing a contract or renewing an unreviewed contract with a vendor.</td>
</tr>
<tr>
<td>Regulated Data Security Controls</td>
<td>Implement PCI DSS [6], HIPAA [7] or export controls as applicable.</td>
</tr>
</tbody>
</table>

**Last Reviewed:** 08/17  
**Document Type:** Standard  
**Applicable To:** Duke University  
**Source URL:** https://security.duke.edu/policies/minimum-security-standards-applications

**Links**  
[1] https://security.duke.edu/policies/minimum-security-standards-applications  