Handheld Hardening Checklists

The hardening checklists are based on the comprehensive checklists produced by The Center for Internet Security (CIS), when possible. The Information Security Office has distilled the CIS lists down to the most critical steps for your systems, with a particular focus on configuration issues that are unique to the computing environment at The University of Texas at Austin.

How to use the checklists

Print the checklist and check off each item you complete to ensure that you cover the critical steps for securing your server. The Information Security Office uses this checklist during risk assessments as part of the process to verify that servers are secure.

How to read the checklists

Step - The step number in the procedure. If there is a UT Note for this step, the note number corresponds to the step number.
Check () - This is for administrators to check off when she/he completes this portion.
To Do - Basic instructions on what to do to harden the respective system.
CIS - Reference number in the The Center for Internet Security (CIS) benchmarks. The CIS documents outline in much greater detail how to complete each step.
UT Note - The notes at the bottom of the pages provide additional detail about the step for the university computing environment.
Cat I - For systems that include category I data, required steps are denoted with the ! symbol. All steps are recommended.
Cat II/III - For systems that include category II or III data, all steps are recommended, and some are required (denoted by the !).

Checklists

<table>
<thead>
<tr>
<th>Handheld device operating systems</th>
<th>Apple iOS Hardening Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Google Android Hardening Checklist</td>
</tr>
</tbody>
</table>