

# CAP SERVER IMPLEMENTATION CHECKLIST

## Summary

CAP servers will be required to access the MnSCU Oracle REPL database after 12/31/06. This checklist of tasks needs to be accomplished for the implementation of a CAP server. Please refer to <http://www.its.mnscu.edu/security/standardsguidelines/index.html> for more details.

## Implementation Check List

MnSCU ITS	Campus	TASK
	<input type="checkbox"/>	<b>1. Network Segmentation</b> – refer to: <a href="http://www.its.mnscu.edu/security/standardsguidelines/networksegstandard523D.pdf">http://www.its.mnscu.edu/security/standardsguidelines/networksegstandard523D.pdf</a>
		a. Map network
		b. Determine logical network segments
		c. Determine where the CAP server will reside
		d. Segment network
		i. Configure campus firewalls
	<input type="checkbox"/>	<b>2. Data Flow Restrictions</b>
		a. CAP server to Oracle databases (permit TCP 1707)
		b. CAP server to anywhere else (permit only for patch and virus updates)
		c. Internet to CAP server (none permitted)
		d. Administrators to CAP server (HTTPS, RDP, ICA)
		e. Non-Admin, students, or public to CAP server (none permitted)
	<input type="checkbox"/>	<b>3. Secure Oracle REPL database access</b>
		a. Identify server to be used as CAP server
		i. Purchase system if necessary
		ii. This can be a shared system with another campus ( <i>Configuration still being defined</i> )
	<input type="checkbox"/>	b. Configure CAP Server - for sizing information refer to: <a href="http://www.its.mnscu.edu/security/standardsguidelines/cap/caparchguidelines.html#Sizing_Guidelines">http://www.its.mnscu.edu/security/standardsguidelines/cap/caparchguidelines.html#Sizing_Guidelines</a>
		i. Anti-virus with logging
		ii. Automated patch management (semi-automated acceptable)
		iii. Define as protected
		iv. Cannot directly access the Internet
		v. Cannot be directly accessible from the Internet
		vi. Protocols restricted to HTTPS, RDP, ICA (TLS-enabled RDP and SecureICA are strongly encouraged)
		vii. Must have a mechanism to log access
		viii. Restricted to data access applications only
		ix. Users accessing Oracle REPL via CAP servers must not have Administrator or system privileges on CAP server
	<input type="checkbox"/>	<b>4. Document Configuration</b>
		a. Document network access rules
	<input type="checkbox"/>	b. Submit completed documentation for review to <a href="mailto:hostmaster@mnscu.edu">hostmaster@mnscu.edu</a>
<input type="checkbox"/>	<input type="checkbox"/>	c. Obtain certification for CAP server connectivity
	<input type="checkbox"/>	<b>5. Implement CAP server</b>
<input type="checkbox"/>		a. MnSCU ITS to open firewall ports for REPL database access
<input type="checkbox"/>	<input type="checkbox"/>	b. Test, test, test!
<input type="checkbox"/>		<b>6. Coordinate Hand Off to Data Warehouse Team</b>