

Title: **Security Profiles**

Date:

Area / Unit	System Environment					
	Development	QA	System Certification	FOA/Beta	Staging	Production
Sustaining Development	RW	RO	RO	RO	RO	None
Advanced Development	RW	RO	RO	RO	RO	None
Strategic Development	RW	RO	RO	RO	RO	None
Quality Assurance	Applications	RW	RO	RO	RO	None
	Databases	RO	RO	RO	RO	RO
Systems Engineering	Applications	RO	RO	RO	RO	RO
	Databases	Exception	Exception	Exception	Exception	Exception
	Hardware	Full	Full	Full	Full	Exception
MIS Database	RO	RO	RO	RO	RO	RO

ICST Internal Departments

Content (Content Utilities)	None	None	None	None	W *	W
Technical Support	None	None	None	SU	SU	SU

External Entities

Exodus	None	None	None	Full	Full	Full
CTC Communications	None	None	None	Full	None	Full

Legend: RW = Read / Write
 RO = Read Only
 Full = Unrestricted
 Exception = Full access with use restricted to request fulfillment
 W = Write (Direct write of Content to Production Database)
 W* = Write (Direct write of Content to Staging Database with automatic content update to the production environment.)
 SU = Super User Utility to assist Web users with ID issues. Audited through review of database logs.
 None = Standard Web access only. No access to applications, databases or hardware.

Note: Sandbox environments are excluded from this procedure. Owners have control over their own environments.

Monitoring of direct content writes to production is required.

Area	Access Areas			
	Servers	Resonate	Database	Network / H/W
Network	X	-	-	-
DBAs	-	-	X	-
OCC	X	-	-	-
Release Engineering	X	-	-	-
Ops Engineering	X	X	-	-
Ops Management	X	X	X	X

Legend: X = Normal access rights for individual trained and demonstrating skills
 - = Situational exceptions requiring security to be enabled. Individuals may act in the capacity of a backup for the primary individual without being a member of the specific area.