MSSEI Data protection profiles

https://security.berkeley.edu/mssei

Information Security and Policy - May 6, 2014

√ = required **+** = recommended (future requirement) **o** = recommended (best practice, strongly encouraged)

Data Class (protection level) / Device/use categories	Level 1			Level 2			Main Actors				
	Individual	Privileged	Institutional	Individual	Privileged	Institutional	User	Image	Proprietor	App Devlpr	Sys Admin
Minimum Security Standard for Electronic Information (MSSEI)											
1.1 Removal of non-required covered data	o	√	√	√	√	√	*		*	*	*
1.2 Covered system inventory		√	√		√	√			*		*
1.3 Covered system registration		+	√		√	√			*		*
1.4 Annual inventory and registration renewal		√	√		√	√			*		*
2.1 Managed software inventory		+	√	o	√	√		*			*
3.1 Secure device configurations	o	+	√	√	√	√		*			*
4.1 Continuous vulnerability assessment/remediation		+	√		√	√					*
4.2 Authenticated scan					√	√				*	*
4.3 Intrusion Detection		+	+		√	√					*
5.1 Device physical security	o	o	+	o	o	√	*				*
6.1 Secure coding training	√	√	√	√	√	√				*	
6.2 Code review						√				*	
6.3 Application security testing						√				*	
6.4 Commercial software assessment						√			*		
7.1 No mobile/wireless "Institutional" devices			+			√				*	*
8.1 Privacy and security training	o	+	+	√	√	√	*		*	*	*
9.1 Unique passphrases	√	√	√	√	√	√	*		*		
9.2 Separation of accounts	√	√	√	√	√	√					*
9.3 Separation of system resources			√			√					*
10.1 Use of admin accounts only on secure devices		+	√		√	√				*	*
10.2 Admin account security		+	√		√	√					
11.1 Managed hardware firewall			√			√					*
11.2 Protected subnets			+			√					*
12.1 Security audit logging			√			√					*
12.2 Security audit log analysis			+			√					*
13.1 Controlled access based on the need to know	√	√	√	√	√	√	*		*		
14.1 Account monitoring and management			√	√	√	√			*		
15.1 Encryption in transit	√	√	√	√	√	√				*	*
15.2 Encryption on mobile devices/removable storage			√	√	√	√	*	*			
15.3 Secure deletion upon decommission	o	√	√	√	√	√		*			
15.4 Data access agreement			√			√			*		*
16.1 Incident response planning			√			√			*		*
16.2 Incident response plan availability			+			√			*		*
16.3 Incident response training	√	√	√	√	√	√			*		*
17.1 MSSND Compliance (see below)	√	√	√	√	√	√					
MSSND											
ND-1 Software patch updates	√	√	√	√	√	√		*			*
ND-2 Anti-malware Software	√	√	√	√	√	√		*			*
ND-3 Host-based Firewall software	√	√	√	√	√	√		*			*
ND-4 Use of authentication	√	√	√	√	√	√	*			*	*
ND-5 Passphrase complexity	√	√	√	√	√	√	*			*	
ND-6 Encrypted authentication	√	√	√	√	√	√			*		*
ND-7 No unattended console sessions	√	√	√	√	√	√	*	*	*		*
ND-8 No unnecessary services	√	√	√	√	√	√		*			*
ND-9 Privileged accounts	√	√	√	√	√	√			*		*

Level 1: Individual
- Devices processing, storing or transmitting protection level 1 data, provided these devices cannot be classified as either institutional or privileged access. **[By default, all Univ. issued employee workstations/ laptops/tablets/ smart phones]**

Level 1: Privileged
- Any device where credentials are used to provide privileged access (super user, root, administrator, database administrator, and equivalent) to an institutional protection level 1 device (physical, logical, and virtual devices included).

Level 1: Institutional
- Servers (i.e., devices that provide access to data from other devices) that store, process or transmit 1,000 or more records of structured or unstructured protection level 1 data. This includes database servers, application servers, web front-end servers, back-up and storage systems, and any systems that provide authentication, authorization, or configuration management for those systems.

OR
- Systems with stored credentials to access protection level 1 data in any of the above systems.

Level 2: Individual
- Devices accessing data in a protection level 2 information system or otherwise processing, storing or transmitting protection level 2 data, provided these end-user devices cannot be classified as either institutional or privileged access.

Level 2: Privileged
- Any device where credentials are used to provide privileged access (super user, root, administrator, database administrator, and equivalent) to an institutional use data protection level 2 device (physical, logical, and virtual devices included).

Level 2: Institutional
- Stores of 500 or more records of structured or unstructured protection level 2 data.

OR
- Servers (i.e., devices that provide access to data from other devices) that store, process or transmit protection level 2 data. This includes database servers, application servers, web front-end servers, back-up and storage systems, and any systems that provide authentication, authorization, or configuration management for those systems.

The "main actor" indicators identify the controls most relevant to a given role. However, **Proprietors** are responsible for partnering with their Resource Custodians to achieve compliance with **all** MSSEI and MSSND controls.

In the absence of an identified IT custodian, **users** are the default custodians for the devices they use.