

	Department of Human Services Online Directives Information System	Index: Effective: Review:	MAN1900 11/01/2014 11/01/2014
---	--	--	--

MANUAL

SUBJECT: Information Security Policies, Procedures and Guidelines

TABLE OF CONTENTS

[Information Security Program & Administrative Controls](#)

[DHS Information Security Glossary](#)

Section #	Titles
Section 100	<u>Information Security Policy</u>
Section 200	<u>Access Control Policy</u>
	<i>Procedures and Guidelines</i>
201	<u>Access Control Procedures</u>
202	<u>Information Asset Ownership</u>
203	<u>Criteria for Access to Information Assets</u>
204	<u>User Identification</u>
205	<u>Generic User IDs</u>
206	<u>Administrator User IDs</u>
207	<u>Inbound and Outbound Access</u>
208	<u>Firewall Maintenance & Management</u>
209	<u>Firewall Failover</u>
210	<u>Physical Firewall Security</u>
211	<u>Firewall Administration</u>
212	<u>Firewall Platform Operating System Builds</u>
213	<u>Firewall Logging</u>
214	<u>Firewall Configuration Backups</u>
215	<u>E-mail – DHR or State Hosting</u>
216	<u>E-mail – Personal Accounts</u>
217	<u>Instant Messaging</u>
218	<u>Logging and Auditing</u>
219	<u>Information Asset Accountability</u>
220	<u>Information Classification/Categorization and Protection</u>
221	<u>Secure Disposal and Re-Use of Information Assets</u>

Section 300	<u>Password Policy</u>
Section 400	<u>USB Purchase and Usage Policy</u>
Section 500	<u>Acceptable Use Policy</u>
	<i>Procedures and Guidelines</i>
501	<u>E-mail and Internet Use</u>
502	<u>Mobile Computing</u>
503	<u>Expectation of Privacy</u>
Section 600	<u>Audit and Accountability Policy</u>
	<i>Procedures and Guidelines</i>
601	<u>Audit Trail Procedures</u>
602	<u>Analysis of Audit Trails</u>
603	<u>Logging and Auditing</u>
Section 700	<u>Configuration Management Policy</u>
	<i>Procedures and Guidelines</i>
701	<u>Change Management Procedures</u>
702	<u>Change Management Process for Information Assets</u>
703	<u>Change Control</u>
704	<u>Change Control Procedures</u>
705	<u>Review of Operating System Changes</u>
706	<u>Restrictions on Changes to Software Packages</u>
Section 800	<u>Contingency Planning Policy</u>
	<i>Procedures and Guidelines</i>
801	<u>Initiating the Business Continuity Plan (BCP) Project</u>
802	<u>Assessing the BCP Security Risks</u>
803	<u>Developing the BCP</u>
804	<u>Testing the BCP</u>
805	<u>Training and Staff Awareness on BCP</u>
806	<u>Maintaining and Updating the BCP</u>
807	<u>Disaster Recovery Plan</u>
Section 900	<u>Identification and Authentication Policy</u>
	<i>Procedures and Guidelines</i>
901	<u>Identification and Authentication Procedures</u>
902	<u>Application Permissions</u>
903	<u>End-User Authentication</u>

Section 1000	<u>Incident Response and Reporting Policy</u>
	<i>Procedures and Guidelines</i>
1001	<u>Incident Response Management and Reporting Plan Procedures</u>
1002	<u>Security Incidents, Incident Reporting, and Incident Management</u>
1003	<u>Firewall Incidents</u>
Section 1100	<u>Information Management Policy</u>
	<i>Procedures and Guidelines</i>
1004	<u>Records Management</u>
1005	<u>Managing Onsite Data Stores</u>
Section 1200	<u>Media Protection Policy</u>
	<i>Procedures and Guidelines</i>
1006	<u>Information Media Handling</u>
1007	<u>Security of Media in Physical Transit</u>
Section 1300	<u>Personnel Security Policy</u>
	<i>Procedures and Guidelines</i>
1008	<u>Position Categorization</u>
1009	<u>Job Descriptions</u>
1010	<u>Segregation of Duties</u>
1011	<u>Background Checks</u>
Section 1400	<u>Physical Environmental Protection Policy</u>
	<i>Procedures and Guidelines</i>
1012	<u>Physical and Environmental Security procedures</u>
1013	<u>Physical and Environmental Security</u>
1014	<u>Facility Access and Employee Identification</u>
1015	<u>Challenging Strangers on the Premises</u>
1016	<u>Physical Protection of Information Assets</u>
Section 1500	<u>Secure Disposal and Re-use of Information Assets Policy</u>
	<i>Procedures and Guidelines</i>
1017	<u>Safeguarding Personal Information Data Procedures</u>
Section 1600	<u>Security Assessment and Authorization Policy</u>

Section 1700	<u>Security Awareness and Training policy</u>
	<i>Procedures and Guidelines</i>
1701	<u>IT Security Awareness training procedure</u>
Section 1800	<u>Security Planning Policy</u>
Section 1900	<u>System and Communications Protection Policy</u>
	<i>Procedures and Guidelines</i>
1702	<u>Electronic Communication</u>
1703	<u>Portable Information System Security</u>
1704	<u>Controls Against Malicious Software</u>
1705	<u>Cryptographic Controls</u>
1706	<u>Communications Service Providers Outside State Government</u>
1707	<u>Remote Access to the DHR Information Infrastructure</u>
1708	<u>Wireless Networks</u>
1709	<u>Onsite Computing</u>
1710	<u>Teleworking</u>
1711	<u>Internet Access to and or from the DHS Infrastructure</u>
1712	<u>Layered Protection Methodology of Information Architecture</u>
Section 2000	<u>System and Information Integrity Policy</u>
Section 2100	<u>System and Services Acquisition Policy</u>
	<i>Procedures and Guidelines</i>
1713	<u>Vendor Services & Products Questionnaire</u>
Section 2200	<u>System Maintenance Policy</u>
	<i>Procedures and Guidelines</i>
2201	<u>System Maintenance procedures</u>
2202	<u>Separation of Development and Production Environments</u>
2203	<u>Scheduled Maintenance, Updates, Patches, and Service Packs</u>
2204	<u>Emergency Maintenance</u>
2205	<u>Clock Synchronization</u>
2206	<u>System Acceptance</u>
2207	<u>Application Permissions</u>
2208	<u>Segregation of Duties</u>
2209	<u>Application Development Environments</u>
2210	<u>Coding Standards and Code Review</u>
2211	<u>System Passwords</u>
2212	<u>Root Access</u>
2213	<u>Application Supporting Architecture</u>
2214	<u>Security Requirements Analysis and Specification</u>

2215 [Data Validation](#)
2216 [Control of Operational Software](#)
2217 [Protection of System Test Data](#)
2218 [Access Control in Program Source Libraries](#)

Section 2300 **[System Security Categorization policy](#)**

Procedures and Guidelines

2301 [System Security Categorization procedures](#)

Section 2400 **[Vulnerability and Risk Assessment Policy](#)**

Procedures and Guidelines

2401 [Vulnerability and Risk Assessments procedures](#)

2402 [Penetration Testing](#)

2403 [Vulnerability and Risk Assessments](#)

Section 2500 **[Compliance](#)**

Procedures and Guidelines

2501 [Compliance Requirements](#)

2502 [Waivers to Security Standards and Guidelines](#)