



Criminal Justice Information Services (CJIS) Security Policy

Version 5.9
06/01/2020

CJISD-ITS-DOC-08140-5.9



Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

TABLE OF CONTENTS

Executive Summary	i
Change Management	ii
Summary of Changes	iii
Table of Contents	iv
List of Figures	ix
1 Introduction	1
1.1 Purpose	1
1.2 Scope	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document	2
1.5 Distribution of the CJIS Security Policy	2
2 CJIS Security Policy Approach	3
2.1 CJIS Security Policy Vision Statement	3
2.2 Architecture Independent	3
2.3 Risk Versus Realism	3
3 Roles and Responsibilities	4
3.1 Shared Management Philosophy	4
3.2 Roles and Responsibilities for Agencies and Parties	4
3.2.1 CJIS Systems Agencies (CSA)	5
3.2.2 CJIS Systems Officer (CSO)	5
3.2.3 Terminal Agency Coordinator (TAC)	6
3.2.4 Criminal Justice Agency (CJA)	6
3.2.5 Noncriminal Justice Agency (NCJA)	6
3.2.6 Contracting Government Agency (CGA)	7
3.2.7 Agency Coordinator (AC)	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)	7
3.2.9 Local Agency Security Officer (LASO)	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)	8
3.2.11 Repository Manager	9
3.2.12 Compact Officer	9
4 Criminal Justice Information and Personally Identifiable Information	10
4.1 Criminal Justice Information (CJI)	10
4.1.1 Criminal History Record Information (CHRI)	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information	11
4.2.1 Proper Access, Use, and Dissemination of CHRI	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	11
4.2.3.1 For Official Purposes	11
4.2.3.2 For Other Authorized Purposes	12
4.2.3.3 CSO Authority in Other Circumstances	12
4.2.4 Storage	12
4.2.5 Justification and Penalties	12

4.2.5.1	Justification	12
4.2.5.2	Penalties	12
4.3	Personally Identifiable Information (PII).....	12
5	Policy and Implementation	14
5.1	Policy Area 1: Information Exchange Agreements	15
5.1.1	Information Exchange	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements	15
5.1.1.3	Criminal Justice Agency User Agreements	16
5.1.1.4	Interagency and Management Control Agreements	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements	17
5.1.1.7	Outsourcing Standards for Channelers	17
5.1.1.8	Outsourcing Standards for Non-Channelers	18
5.1.2	Monitoring, Review, and Delivery of Services	18
5.1.2.1	Managing Changes to Service Providers	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI	18
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Basic Security Awareness Training	20
5.2.1.1	Level One Security Awareness Training	20
5.2.1.2	Level Two Security Awareness Training	20
5.2.1.3	Level Three Security Awareness Training	21
5.2.1.4	Level Four Security Awareness Training	21
5.2.2	LASO Training.....	22
5.2.3	Security Training Records.....	22
5.3	Policy Area 3: Incident Response	24
5.3.1	Reporting Security Events.....	24
5.3.1.1	Reporting Structure and Responsibilities.....	24
5.3.1.1.1	FBI CJIS Division Responsibilities	24
5.3.1.1.2	CSA ISO Responsibilities.....	24
5.3.2	Management of Security Incidents.....	25
5.3.2.1	Incident Handling.....	25
5.3.2.2	Collection of Evidence.....	25
5.3.3	Incident Response Training.....	25
5.3.4	Incident Monitoring.....	25
5.4	Policy Area 4: Auditing and Accountability.....	27
5.4.1	Auditable Events and Content (Information Systems).....	27
5.4.1.1	Events.....	27
5.4.1.1.1	Content.....	28
5.4.2	Response to Audit Processing Failures	28
5.4.3	Audit Monitoring, Analysis, and Reporting.....	28
5.4.4	Time Stamps.....	28
5.4.5	Protection of Audit Information	28
5.4.6	Audit Record Retention.....	28
5.4.7	Logging NCIC and III Transactions.....	29

5.5	Policy Area 5: Access Control.....	30
5.5.1	Account Management	30
5.5.2	Access Enforcement.....	30
5.5.2.1	Least Privilege	31
5.5.2.2	System Access Control	31
5.5.2.3	Access Control Criteria.....	31
5.5.2.4	Access Control Mechanisms.....	31
5.5.3	Unsuccessful Login Attempts	32
5.5.4	System Use Notification.....	32
5.5.5	Session Lock	32
5.5.6	Remote Access	33
5.5.6.1	Personally Owned Information Systems.....	33
5.5.6.2	Publicly Accessible Computers	33
5.6	Policy Area 6: Identification and Authentication	35
5.6.1	Identification Policy and Procedures.....	35
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges	35
5.6.2	Authentication Policy and Procedures	35
5.6.2.1	Standard Authenticators.....	36
5.6.2.1.1	Password	36
5.6.2.1.2	Personal Identification Number (PIN)	38
5.6.2.1.3	One-time Passwords (OTP)	38
5.6.2.2	Advanced Authentication.....	38
5.6.2.2.1	Advanced Authentication Policy and Rationale	39
5.6.2.2.2	Advanced Authentication Decision Tree	39
5.6.3	Identifier and Authenticator Management	41
5.6.3.1	Identifier Management.....	41
5.6.3.2	Authenticator Management.....	42
5.6.4	Assertions	42
5.7	Policy Area 7: Configuration Management	48
5.7.1	Access Restrictions for Changes	48
5.7.1.1	Least Functionality.....	48
5.7.1.2	Network Diagram.....	48
5.7.2	Security of Configuration Documentation	48
5.8	Policy Area 8: Media Protection.....	49
5.8.1	Media Storage and Access	49
5.8.2	Media Transport	49
5.8.2.1	Digital Media during Transport	49
5.8.2.2	Physical Media in Transit	49
5.8.3	Digital Media Sanitization and Disposal.....	49
5.8.4	Disposal of Physical Media.....	49
5.9	Policy Area 9: Physical Protection	51
5.9.1	Physically Secure Location	51
5.9.1.1	Security Perimeter.....	51
5.9.1.2	Physical Access Authorizations	51
5.9.1.3	Physical Access Control	51

5.9.1.4	Access Control for Transmission Medium	51
5.9.1.5	Access Control for Display Medium	51
5.9.1.6	Monitoring Physical Access	52
5.9.1.7	Visitor Control	52
5.9.1.8	Delivery and Removal	52
5.9.2	Controlled Area	52
5.10	Policy Area 10: System and Communications Protection and Information Integrity	53
5.10.1	Information Flow Enforcement	53
5.10.1.1	Boundary Protection	53
5.10.1.2	Encryption.....	54
5.10.1.2.1	Encryption for CJI in Transit	54
5.10.1.2.2	Encryption for CJI at Rest.....	55
5.10.1.2.3	Public Key Infrastructure (PKI) Technology.....	55
5.10.1.3	Intrusion Detection Tools and Techniques	55
5.10.1.4	Voice over Internet Protocol.....	56
5.10.1.5	Cloud Computing.....	56
5.10.2	Facsimile Transmission of CJI.....	57
5.10.3	Partitioning and Virtualization	57
5.10.3.1	Partitioning.....	57
5.10.3.2	Virtualization	58
5.10.4	System and Information Integrity Policy and Procedures.....	58
5.10.4.1	Patch Management.....	58
5.10.4.2	Malicious Code Protection.....	59
5.10.4.3	Spam and Spyware Protection	59
5.10.4.4	Security Alerts and Advisories	59
5.10.4.5	Information Input Restrictions.....	60
5.11	Policy Area 11: Formal Audits	61
5.11.1	Audits by the FBI CJIS Division.....	61
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division	61
5.11.1.2	Triennial Security Audits by the FBI CJIS Division	61
5.11.2	Audits by the CSA.....	61
5.11.3	Special Security Inquiries and Audits	62
5.11.4	Compliance Subcommittees	62
5.12	Policy Area 12: Personnel Security	63
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI	63
5.12.2	Personnel Termination	64
5.12.3	Personnel Transfer.....	64
5.12.4	Personnel Sanctions.....	64
5.13	Policy Area 13: Mobile Devices	66
5.13.1	Wireless Communications Technologies	66
5.13.1.1	802.11 Wireless Protocols	66
5.13.1.2	Cellular Devices.....	67
5.13.1.2.1	Cellular Service Abroad.....	68
5.13.1.2.2	Voice Transmissions Over Cellular Devices	68
5.13.1.3	Bluetooth.....	68

5.13.1.4	Mobile Hotspots.....	68
5.13.2	Mobile Device Management (MDM)	69
5.13.3	Wireless Device Risk Mitigations	69
5.13.4	System Integrity	70
5.13.4.1	Patching/Updates	70
5.13.4.2	Malicious Code Protection.....	70
5.13.4.3	Personal Firewall	70
5.13.5	Incident Response	71
5.13.6	Access Control	71
5.13.7	Identification and Authentication.....	71
5.13.7.1	Local Device Authentication	71
5.13.7.2	Advanced Authentication.....	72
5.13.7.2.1	Compensating Controls.....	72
5.13.7.3	Device Certificates.....	72
Appendices.....		A-1
Appendix A	Terms and Definitions	A-1
Appendix B	Acronyms.....	B-1
Appendix C	Network Topology Diagrams	C-1
Appendix D	Sample Information Exchange Agreements.....	D-1
D.1	CJIS User Agreement	D-1
D.2	Management Control Agreement.....	D-9
D.3	Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4	Interagency Connection Agreement	D-16
Appendix E	Security Forums and Organizational Entities.....	E-1
Appendix F	Sample Forms.....	F-1
F.1	Security Incident Response Form	F-2
Appendix G	Best practices.....	G-1
G.1	Virtualization	G-1
G.2	Voice over Internet Protocol.....	G-4
G.3	Cloud Computing.....	G-15
G.4	Mobile Appendix	G-32
G.5	Administrator Accounts for Least Privilege and Separation of Duties.....	G-53
G.6	Encryption.....	G-66
G.7	Incident Response	G-76
G.8	Secure Coding.....	G-89
Appendix H	Security Addendum	H-1
Appendix I	References.....	I-1
Appendix J	Noncriminal Justice Agency Supplemental Guidance	J-1
Appendix K	Criminal Justice Agency Supplemental Guidance	K-1

LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components.....	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department	19
Figure 4 – Security Awareness Training Use Cases.....	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department	26
Figure 6 – Local Police Department's Use of Audit Logs	29
Figure 7 – A Local Police Department's Access Controls	34
Figure 8 – Advanced Authentication Use Cases.....	42
Figure 9 – Authentication Decision for Known Location	46
Figure 10 – Authentication Decision for Unknown Location	47
Figure 11 – A Local Police Department's Configuration Management Controls	48
Figure 12 – A Local Police Department's Media Management Policies.....	50
Figure 13 – A Local Police Department's Physical Protection Measures.....	52
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	60
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls	64