SAFE-AI

AI Controls

This table contains a list of 100 NIST SP 800 Rev 5 controls that should be included in SSPs for AI-enabled systems. Modifying control descriptions in the SSP may be warranted for addressing specific weaknesses. The table includes four columns indicating the relation between AI controls and the four system elements of an AI-enabled system as defined here:

- Environment – infrastructure, network
- AI Platform – AI components, software
- AI Models – ML models, LLMs
- AI Data – training data, validation data

Table 1 - AI Controls

Control ID	Control Name	Environment	AI Platform	AI Models	AI Data	NIST baseline
AC-01-00	Policy and Procedures	X	X			LMH
AC-02-12	Account Management | Account Monitoring for Atypical Usage	X	X			H
AC-03-00	Access Enforcement	X	X	X	X	LMH
AC-04-00	Information Flow Enforcement	X	X	X	X	MH
AC-04-09	Information Flow Enforcement | Human Reviews		X			
AC-04-15	Information Flow Enforcement | Detection of Unsanctioned Information		X			
AC-04-25	Information Flow Enforcement | Data Sanitization	X	X	X	X	
AC-05-00	Separation of Duties	X	X	X		MH
AC-06-00	Least Privilege	X	X	X	X	MH
AC-07-00	Unsuccessful Logon Attempts	X	X			LMH
AC-12-00	Session Termination		X			MH
AC-14-00	Permitted Actions Without Identification or Authentication	X	X		X	LMH
AC-17-00	Remote Access	X	X			LMH
AC-20-00	Use of External Systems	X	X	X	X	LMH
AC-21-00	Information Sharing	X	X		X	MH
AC-23-00	Data Mining Protection		X			
AC-24-00	Access Control Decisions	X	X			
AT-03-00	Role-based Training			X	X	LMH
AU-02-00	Event Logging	X	X	X		LMH
AU-03-00	Content of Audit Records			X		LMH
AU-06-00	Audit Record Review, Analysis, and Reporting	X	X			LMH

SAFE-AI

Control ID	Control Name	Environment	AI Platform	AI Models	AI Data	NIST baseline
AU-06-05	Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records	X	X			H
AU-09-00	Protection of Audit Information		X		X	LMH
CA-02-00	Control Assessments	X	X	X	X	LMH
CA-08-00	Penetration Testing	X	X			H
CA-09-00	Internal System Connections	X				LMH
CM-02-00	Baseline Configuration		X	X	X	LMH
CM-03-00	Configuration Change Control	X	X			MH
CM-05-00	Access Restrictions for Change	X	X	X		LMH
CM-07-00	Least Functionality	X	X	X	X	LMH
CM-11-00	User-installed Software	X	X			LMH
CM-13-00	Data Action Mapping		X			
CM-14-00	Signed Components	X	X			
CP-01-00	Policy and Procedures	X	X			LMH
CP-09-00	System Backup	X	X	X	X	LMH
IA-02-00	Identification and Authentication (organizational Users)	X	X			LMH
IA-02-01	Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts	X	X			LMH
IA-02-02	Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts	X	X			LMH
IA-03-00	Device Identification and Authentication	X				MH
IA-06-00	Authentication Feedback	X				LMH
IA-08-00	Identification and Authentication (non-organizational Users)	X	X			LMH
IA-12-00	Identity Proofing	X	X			MH
MA-03-00	Maintenance Tools	X	X			MH
MA-05-00	Maintenance Personnel	X	X			LMH
MA-06-00	Timely Maintenance	X	X			MH
PE-11-00	Emergency Power	X				MH
PL-02-00	System Security and Privacy Plans		X	X	X	LMH
PL-04-00	Rules of Behavior		X	X	X	LMH
PL-08-00	Security and Privacy Architectures	X				MH
PM-07-00	Enterprise Architecture	X				LMH
PM-12-00	Insider Threat Program	X	X	X	X	LMH
PM-18-00	Privacy Program Plan	X				LMH
PM-30-00	Supply Chain Risk Management Strategy			X		LMH
RA-03-00	Risk Assessment	X	X			LMH
RA-05-00	Vulnerability Monitoring and Scanning	X	X			LMH

SAFE-AI

Control ID	Control Name	Environment	AI Platform	AI Models	AI Data	NIST baseline
SA-03-02	System Development Life Cycle | Use of Live or Operational Data		X		X	
SA-08-00	Security and Privacy Engineering Principles		X			LMH
SA-09-00	External System Services		X		X	LMH
SA-09-05	External System Services | Processing, Storage, and Service Location				X	
SA-09-06	External System Services | Organization-controlled Cryptographic Keys				X	
SA-09-08	External System Services | Processing and Storage Location — U.S. Jurisdiction				X	
SA-10-00	Developer Configuration Management		X	X	X	MH
SA-17-00	Developer Security and Privacy Architecture and Design		X			H
SA-22-00	Unsupported System Components	X	X			LMH
SC-02-00	Separation of System and User Functionality	X	X			MH
SC-03-00	Security Function Isolation	X	X			H
SC-04-00	Information in Shared System Resources	X	X	X	X	MH
SC-05-00	Denial-of-service Protection	X	X			LMH
SC-06-00	Resource Availability	X	X			
SC-07-00	Boundary Protection	X				LMH
SC-08-00	Transmission Confidentiality and Integrity	X	X	X	X	MH
SC-10-00	Network Disconnect		X			MH
SC-12-00	Cryptographic Key Establishment and Management			X		LMH
SC-13-00	Cryptographic Protection				X	LMH
SC-15-00	Collaborative Computing Devices and Applications		X			LMH
SC-17-00	Public Key Infrastructure Certificates				X	MH
SC-18-00	Mobile Code		X			MH
SC-23-00	Session Authenticity	X	X			MH
SC-24-00	Fail in a Known State		X	X		H
SC-28-00	Protection of Information at Rest	X	X	X	X	MH
SC-37-00	Out-of-band Channels	X	X			
SC-39-00	Process Isolation	X	X			LMH
SI-02-00	Flaw Remediation	X	X			LMH
SI-03-00	Malicious Code Protection	X	X	X	X	LMH
SI-04-00	System Monitoring	X	X	X	X	LMH
SI-05-00	Security Alerts, Advisories, and Directives	X	X			LMH
SI-07-00	Software, Firmware, and Information Integrity	X	X	X	X	MH
SI-10-00	Information Input Validation		X	X	X	MH
SI-11-00	Error Handling		X			MH
SI-16-00	Memory Protection	X	X			MH

SAFE-AI

Control ID	Control Name	Environment	AI Platform	AI Models	AI Data	NIST baseline
SI-20-00	Tainting			X	X	
SR-01-00	Policy and Procedures		X	X	X	LMH
SR-02-00	Supply Chain Risk Management Plan			X	X	LMH
SR-03-00	Supply Chain Controls and Processes	X	X	X	X	LMH
SR-04-00	Provenance		X	X		
SR-05-00	Acquisition Strategies, Tools, and Methods	X	X	X	X	LMH
SR-06-00	Supplier Assessments and Reviews		X	X	X	MH
SR-08-00	Notification Agreements		X	X	X	LMH
SR-09-00	Tamper Resistance and Detection	X	X			H
SR-11-00	Component Authenticity		X			LMH