InCommon Identity Assurance and HEISC Information Security Guide

InCommon IAP and Information Security Guide – a Cross Reference

Link to InCommon Identity Assurance Profiles Bronze and Silver
Link to Information Security Guide

4.2 Specification of Identity Assurance Requirements	Applicable Topics in the Information Security Guide
4.2.1 Business, Policy and Operational Criteria IdP Operators must have the organizational structures and processes to come into and remain in compliance with the provisions of this IAP.	ISO 6: Organization of Information Security
.1 InCommon Participant.	
.2 Notification to InCommon	
.3 Continuing Compliance	ISO 15: Compliance
4.2.2 Registration and Identity Proofing	ISO 8: Human resources Security. Including pre-employment screening procedures ion the Guide could help InCommon participants. Alternatively, the Guide might point to the IAP for identity proofing procedures for onboarding employees. ISO 11: Access control Page 59 of AACRAO Vol. 87 No. 3: Establishing Remote Student Identity would be a useful reference for the Guide. See definitions from the AACRAO article at InCommon Assurance Remote Proofing Definitions and Concepts
.1 RA authentication	
.2 Identity verification process	ISO 11.2: User Access Management
.3 Registration records	ISO 11.1 Business Requirements for Access Control ISO 11.2: User Access Management
.4 Identity proofing	ISO 11.2: User Access Management
.4.1 Existing relationship	ISO 11.2: User Access Management
.4.2 In-person proofing	ISO 11.2: User Access Management
.4.3 Remote proofing	ISO 11.2: User Access Management
.5. Address of Record confirmation	ISO 11.2: User Access Management
4.2.3 Credential Technology	ISO 11.5 Operating System Access Controls
Criteria	
.1 Credential unique identifier	
.2 Resistance to guessing Authentication Secret	
.3 Strong resistance to guessing Authentication Secret	
.4 Stored Authentication Secrets	ISO 12.3 Cryptographic Controls
.5 Protected Authentication Secrets	ISO 12.3 Cryptographic Controls
4.2.4 Credential Issuance and Management	
.1 Credential issuance process	
.2 Credential revocation or expiration	
.3 Credential renewal or re-issuance	
.4 Retention of Credential issuance records	
4.2.5 Authentication Process	ISO 11: Access Control
Criteria	
.1 Resist replay attack	
.2 Resist eavesdropper attack	
.3 Secure communication	ISO 11.4 Network access Control
.4 Proof of Possession	

.5 Session authentication	ISO 11.5 Operating System Access Controls
.6 Mitigate risk of sharing Credentials	ISO 11.5 Operating System Access Controls ISO 11.3: User Responsibilities
4.2.6 Identity Information Management	
Criteria	
.1 Identity record qualification	
4.2.7 Assertion Content	
Criteria	
.1 Identity Attributes	
.2 Identity Assertion Qualifier	
.3 Cryptographic security	ISO 12: Information Systems Acquisition, Development, and Maintenance ISO 12.3 Cryptographic Controls
4.2.8 Technical Environment	ISO 9: Physical and Environmental Security ISO 10: Communications and Operations Management
Criteria	
.1 Software maintenance	ISO 12.6: Technical Vulnerability Management
.2 Network security	ISO 10.6: Network Security Management
.3 Physical security	ISO 9: Physical and Environmental Security
.4 Reliable operations	ISO 10: Communications and Operations Management ISO 10.10 Systems Monitoring