

SAM – INFORMATION SECURITY
(Office of Information Security)

PERSONNEL SECURITY

5320.4

(Revised 12/13)

Policy: Each state entity shall establish processes and procedures to ensure that individual access to information assets is commensurate with job-related responsibilities, and individuals requiring access to information assets sign appropriate user agreements prior to being granted access.

Access agreements shall include acceptable use provisions, and may also include nondisclosure agreements and conflict-of-interest agreements. If required by law, regulation or policy, each state entity must ensure individuals obtain applicable security clearances.

Personnel transfers or reassignments to other positions within the state entity must be reviewed to prevent accumulation of access and support least access privilege. Returning and issuing keys, identification cards, and building passes; closing information system accounts and establishing new accounts; and changing information system access authorizations are all examples of personnel security practices related to staff transfer or reassignment.

Implementation Controls: NIST SP 800-53: [Personnel Security \(PS\)](#)