

FISSA+ Privacy & Records Management

Module 5: Information System Access Best Practices

1	Data owners within the business units have the primary responsibility for determining who can have access to their information.
2	There must be a minimum of one account for each person who uses a computer and only the account owner should use that account and password. Each person is accountable for actions taken under their DOI computer account(s).
3	Passwords are the single greatest vulnerability to breaking into an information system. Use long, complex passwords.
4	Don't use the same passwords for your DOI network accounts and your personal computer accounts.
5	It is YOUR responsibility to maintain the PIV credential and safeguard the card and PIN (Personal Identification Number). Do not delay renewing the PIV card to the last minute.
6	All network activity may be monitored, examined, recorded, copied and escalated as appropriate.
7	Never send sensitive information from your DOI account to personal external accounts, including passwords, work files, and emails with sensitive information.
8	Do not download or install personal or unauthorized applications/devices on federal government computers. Respect intellectual property.
9	Do not use live streaming services for non-work purposes.
10	Do not share your passwords or PIN with anyone else.
11	Whenever using the DOI network, the Warning Banner applies to you and you should review it periodically.