SSRL COMPUTER POLICY

Identification and Authentication Policy (Password Policy)

This policy applies to all personnel that use SSRL information or computer system resources on the SPEAR experimental floor, the SPEAR accelerator, or the SSRL central servers (VMS cluster and SSRL Windows Active Directory).

Group (shared) accounts, are only allowed to be used on controls equipment (consoles). For other non-data-acquisition or equipment or accelerator control work, individual accounts have to be used.

Password Lifetime

Individual accounts have a password lifetime of 6 months. Group (shared) accounts used on the experimental floor and in the accelerator area have a maximum password age of 12 months. These accounts are synchronized to the SPEAR annual run schedule and are changed during the annual accelerator shutdown.

Password Rules

Choose a password which does not reside in any dictionary or in any language.

SSRL Windows Active Directory

- Password must be 8 or more characters in length.
- Password must contain at least three of the four following character sets:
  - Upper case (A-Z)
  - Lower case (a-z)
  - Numeric (0-9)
  - Special characters such as punctuation symbols
- Password must not contain a string derived from your name or userid.

SSRL Central VMS Cluster and SPEAR VMS Cluster

- Password must be between 8 and 32 characters in length.
- Password must contain at least three of the four following character sets:
SSRL central VMS cluster passwords can be changed from interactive sessions using the “SET PASSWORD” command or via https://www-ssrl.slac.stanford.edu/computing/cng/set-password.html

Experimental Floor (VMS)

- Password must be between 8 and 32 characters in length.
- Password must contain all three of the following character sets:
  - Alphabetic characters (A-Z, a-z)
  - Numeric (0-9)
  - Special characters (“$”, “_”).

Experimental Floor (UNIX, Crystallography group)

- Password must be exactly 8 characters in length.
- Password must contain:
  - Both upper and lower case characters (A-Z, a-z)
  - Numeric (0-9) and/or symbolic characters
- Password must not:
  - Contain a dictionary word
  - Significantly resemble an older password

SPEAR UNIX

SLAC Unix policy is applicable.

For additional information regarding SLAC’s general password policy see: http://www2.slac.stanford.edu/computing/security/password/passwordpolicy.htm

The SSRL Enclave CSPP refers to this policy.

Joachim Stöhr
8/8/2007