End User Security Policy

Information Technology Security Policies,

Edition 1.1

Originally By:

Mike McGrath

Fedora Project Infrastructure

mmcgrath@redhat.com

Updated By:

Mark Rosenbaum

Fedora Project Infrastructure

markrosenbaum@fedoraproject.org

Legal Notice

Abstract

This is the official End User security policy for The Fedora Project. Below is a list of chapters for consideration.

End User Security Introduction

Sections:

End user security is a critical aspect of a total security solution. All too often security breaches are the result of human error. Every person involved in an information system must take an active role to ensure their own security and the security of the organization. High levels of technical skill are not required in all cases to maintain a secure environment. This chapter does not focus on technical details such as computer settings. Instead, it focuses on actions that can and should be taken by every individual to maintain a secure working environment.

1. End User Standards

Users who have questions about any of the items below should contact infrastructure@lists.fedoraproject.org for answers. Do not ignore an item because you are confused about its meaning.

Required User Actions

Complete	Requirement	Action	Comment
	Must Not	Password Dissemination	Any passwords must be kept secret, known only to the person who created them. Under no circumstances should a user give a password to anyone, unless required by law enforcement. Discuss with your legal counsel in the event of a required legal dissemination. Passwords should not be given to management, technical professionals, or anyone else who asks for them.
	Must Not	Host authentication	Do not log in to any password- or key-protected services from any hosts that are not your personal workstation or a machine or host run by The Fedora Project.

Must Not	Password Usage	Users must not type their plain text passwords into a file on an unencrypted filesystem. Users must also ensure they do not display their passwords on a terminal using any method that records them to an alternate, unsecured location. If, for some reason, a password is displayed in this way, such as typing the password directly in a shell command, be sure to deactivate the retention of shell history, such as `unset HISTFILE` in the case of the `bash` shell. When using this method, create a new shell, deactivate the shell history retention, run your commands and log out of that shell as soon as possible. Shell history is written at logout time, so you cannot "hide" commands by temporarily turning off shell history retention.
Must	Password Entropy	All passwords must meet all of the following requirements: (1) Passwords must be at least 8 characters long. (2) Each password must have at least 1 numeric character. (3) Each password must have at least 1 lower case letter. (4) Each password must have at least 1 upper case letter. (5) Each password must have at least one non-alphanumeric character in them.
Should	ssh ProxyCommand	When using a gateway or proxy host to access another group of machines from your workstation, the most secure option is to use the `ssh` command's `ProxyCommand` option. Refer to `man ssh_config` for more information on proper setup.
Must	Desktop Locking	Any time you physically leave your workstation or any other host that contains a user input or output device such as a keyboard, mouse, or monitor, either lock the screen or shell, or log out completely.

Should Not	Password Reuse	Avoid reusing passwords in environments where there is not a single sign on capability. This is especially important in the case of password protected keys, encrypted shares, access to sensitive personal sites such as banking or other finances, and so on. Always maintain different passwords wherever possible.
Should Not	Software installation	Users should not install any unapproved software. Contact your helpdesk for more information at infrastructure@lists.fedoraproject.org. Advanced or power users who are running programs or scripts that have not been installed by the helpdesk may be liable for any damage they do. Whenever possible scripts or programs should be run under a freshly created user account with standard privileges, to limit access to sensitive passwords or keys.
Must Not	Relocate information offsite	Information contained on file shares, or in databases on infrastructure servers should be assumed to have a non-shareable license. This information should not be transfered offsite without the express written consent of both admin fedoraproject.org and admin fedoraproject.org, including printed copies or data in any form. Exceptions to this rule may include logs that contain no private information, as defined by the applicable privacy policy.
Must	Key Security	Keys retained on any host must be readable only by the owner or group of that key, and ideally should retain file permissions that allow the user owner to read them, but prevent any other access. In UNIX parlance this is a permission setting of 0400.
Must	Key passwords	All private keys must be encrypted with unique passwords. These passwords must meet the criteria laid out above.

Must	Encryption Backups	Users who use encryption keys must retain backups of those keys in a location that can be taken offline, ideally a USB key or other detachable device. This device must be kept in a secure location and only connected to a host while a backup is being made, or while a key from that device is being used or restored. The filesystem on which this key backup exists should be encrypted.
Must	Stolen or Missing Equipment	Any stolen or missing equpment containing any sensitive data including passwords or keys, whether encrypted or not, must be reported as quickly as possible. When handled expediently, issues due to missing equipment can be easily mitigated.

1.1 Administrative Exceptions

At times, engineers and administrators will need to work in systems where passwords or keys must be shared. In these instances the following exceptions apply.

Required User Actions

Complete	Requirement	Action	Comment
	Must	Password Sharing	When a password is not directly tied to a human-user (for example, a mail management software password or network device password), the shared password must be stored and shared in an encrypted format accessible only by an assigned group. When any user is removed from this group, that password must be changed. Shared passwords should be avoided wherever feasible.
	Must	Role Accounts	Accounts that provide access to resources for purpose of automation or other system related access must be tied to an individual user and not shared. The person associated with that account may change, but no more then one person at a time should be responsible for a role based account.
	Must	Data Access Passwords	Passwords that provide access to data resources, such as a database for a web application, are considered shared passwords. See the exception on "Password Sharing" for details.
	Must Not	Self Access	Administrators and users must not give themselves access to resources unless there is an extant emergency or a setup issue. Follow normal procedures to obtain group membership or sponsorship.

2. Security Incidents

Security incidents are serious matters. Any detection of a security breach or malicious behavior should immediately be reported. Users should contact the security team directly at admin fedoraproject.org. Please do

not share any details related to the incident with anyone other than the initial contact. Maintaining confidentiality protects you and The Fedora Project from further internal attacks. A potential attacker that becomes aware of detection may cover tracks or change behavior suddenly, which makes investigation more difficult. On the other hand, if the security team is aware of and tracking an attack in progress, the chances of catching the attacker greatly increases.

3. External Sources and References

- **Hardening RHEL5**
  http://people.redhat.com/sgrubb/files/hardening-rhel5.pdf
- **CentOS OS_Protection**
  http://wiki.centos.org/HowTos/OS_Protection

Revision History

Revision 1	Wed Apr 28 2010	Mike McGrath

Initial movement from the old publican format to 1.6

Revision 2	Tue Jul 16 2024	Mark Rosenbaum

Recovering document from archive and updating