Purdue Linux Users Group
Linux Mirror Policy

Version 2.21

This document, and all subsequent official versions, is licensed under the Creative Commons Attribution 4.0 International License.

Table of Contents

Forward & Statement of Purpose....2
Definitions....3
Mirror change policy....4
  Supported projects and mirror policy....4
  Addition/removal of PLUG mirror maintainers....4
Information Access & Control....6
  Supported protocols....6
  Encryption standards....6
Public mirror information....9
  Public disclosure of policies....9
  Information disclosure canary....9
  Users with additional, non-standard access to the mirror....9
  Contact methods for Mirror Maintainers & RCAC personnel with access to the mirror....10
  Internal mirror documentation....10

Forward & Statement of Purpose

"The purpose of PLUG is to further understanding of the Open Source movement, Open Source software, operating systems, development methodologies and related technologies. PLUG is also chartered to provide support for computer-related problems, specifically relating to Open Source software, operating systems, and development. PLUG is also chartered to provide forums, speakers, information, and events to help foster and grow the Open Source community at Purdue." - Purdue Linux Users Group Constitution, rev. 2018-01-08

The PLUG mirror, having been established in the interests of supporting the Purdue Linux Users Group mission, exists to serve both the on-campus and global computing community. In the furtherance of community ideals, it exists to provide a forum for the free exchange of well-known, publicly trusted open source software.

The following core tenet guide mirror policy:

- Reliability – Software should be provided at any time, to anyone, anywhere, insofar as they are able to access the global internet.
- Breadth – Software should be provided for a variety of use cases, both for currently supported and historical systems. Further, software should be made available using a variety of protocols, in order to support a variety of use cases.
- Privacy – Users should be able to download freely available, legal software without fear of being tracked, monitored, sanctioned, or otherwise penalized.
- Integrity – Users should be confident that the software their software has not been modified, tampered with, or otherwise changed by the source that they are downloading it from.
- Trust – Users should be confident that the software they are downloading is being provided in accordance with well-known policies designed to protect their use.

The Purdue Linux Users Group Mirror is made available with with ABSOLUTELY NO WARRANTY OR EXPECTATION OF SERVICE, to the extent permitted by applicable law. The policies outlined in this document shall not be considered a legally binding contract; they are, at best, organizational policies dictating the management of a shared computational resource.

Definitions

Purdue Linux Users Group (PLUG) – the Purdue student-run organization responsible for maintaining the PLUG Linux Mirror.

The Mirror, Mirror, PLUG Mirror – the public-facing computer system operated by the Purdue Linux Users Group and hosted by Purdue RCAC which is designated for use in distributing freely available, open-source software.

Mirror Maintainer(s), PLUG Mirror Maintainer(s) – an individual (or individuals) tasked with assisting the ongoing operations for the Purdue Linux Users Group mirror.

Purdue Research Computing (RCAC) – The Purdue Research Computing department. Part of Purdue's Information Technology Department, RCAC oversees the Purdue computing cluster. RCAC graciously donates hardware and hosting for the PLUG mirror inside of their on-campus datacenter.

Purdue RCAC personnel – individual(s), acting in their official capacities within RCAC, who maintain some level of access to the PLUG mirror. In the event that RCAC personnel are also involved with ongoing mirror maintenance, they shall be classified as a mirror maintainer.

Publicly available (when in reference to materials directly relating to PLUG mirror or its operations) – content that shall be hosted directly on the mirror, available for access by any individual.

Mozilla Server-Side TLS recommendations – a list of TLS configuration recommendations published by the Mozilla foundation, made freely available via the organization's wiki. As of September 14th, 2021, the recommendations may be found here: https://wiki.mozilla.org/Security/Server_Side_TLS

Fully qualified domain name (FQDN) – the complete address of an individual computer. In the instance of PLUG mirror, the official FQDN shall be "plug-mirror.rcac.purdue.edu".

Key words (SHALL, MAY, MUST NOT, SHOULD NOT, etc…) - key words shall be defined as listed in RFC2119 (https://datatracker.ietf.org/doc/html/rfc2119**).**

Shell – an instance of the Bash, ZSH, sh, or other similar software.

Freely available – software that is available free of charge.

Mirror change policy

Supported projects and mirror policy

The PLUG mirror exists to support freely available, open-source projects. Projects which are closed-source, not freely available, or otherwise not in the interest of the greater interests of the PLUG community must not be mirrored by the PLUG mirror.

Projects may be permanently added or removed from the PLUG mirror via any of the following options:

- A majority vote from the current PLUG officers, as determined by current the PLUG club constitution
- A majority vote from all currently serving PLUG mirror maintainers

Projects may be temporarily removed, hidden, disabled, re-routed, or made otherwise unavailable by any mirror maintainer for the purposes of protecting mirror integrity.

Mirror policy must only be changed via a majority vote of the current PLUG officers, as determined by the current PLUG constitution.

Addition/removal of PLUG mirror maintainers

As needed, any member of the Purdue Linux Users Group in good standing (as defined by the current PLUG club constitution) who has received a majority vote of the current PLUG officers (as determined by the current club constitution) may be considered eligible to become a PLUG mirror maintainer.

The individual must:

- Have been an active member of PLUG for at least one year,
- Have demonstrated a commitment to the purpose and ideals of the mirror,
- Be willing and able to meet and uphold the listed security requirements,
- Have demonstrated technical competency with the use of a shell and other critical components of a Linux-based computer system,
- Be willing to post the required contact information publicly, and
- Be willing to respond to mirror stability or security incidents.

Further, the following categorizations, descriptions, and circumstances must not affect an individual's ability to become a maintainer: “Race, religion, color, sex, age, national origin or ancestry, genetic information, marital status, parental status, sexual orientation, gender identity and expression, disability, or status as a veteran” (*exact verbiage as required by Purdue Administration*).

PLUG Mirror maintainers may assist with the mirror so long as they continue to fulfill the aforementioned requirements. Should a maintainer wish to step down from the position, they must be permitted to do so without prejudice.

As a guideline, there should be approximately 5 PLUG mirror maintainers at any given time, at least one of whom should have physical access to the RCAC datacenter. In order to ensure both consistent administration and coherency of teamwork, no more than 6 mirror maintainers may serve at any given time.

Should a maintainer fail to fulfill any of the above guidelines, they may be forcibly removed from the position by a majority vote of the current PLUG officers (as determined by current the PLUG club constitution).

Should any maintainer be subject to a security incident, their access to mirror must be temporarily restricted in accordance with Maintenance Access policies.

Information Access & Control

Supported protocols

All information stored on the PLUG mirror shall be available via all supported protocols. In the event of extenuating circumstances, PLUG mirror maintainers may elect to temporarily disable, throttle, restrict, or otherwise impede access to any supported protocol or information provided therein at their sole discretion.

The following protocols shall be supported via their well-known ports: HTTP, HTTPS, FTP, and RSYNC.

Additional protocols, software, scripts, and tools may be employed by the PLUG mirror maintainers for operational purposes.

Encryption standards

Encrypted protocols must not be given preference over unencrypted protocols. Unencrypted traffic must not be automatically redirected to a encrypted endpoint.

For TLS, the Mozilla Server-Side TLS standards must always be followed. At the discretion of the maintainers, either the Modern or Intermediate configurations may be used.

When public trust is required for TLS, all certificates must be exclusively generated and signed by the Internet Security Research Group (ISRG, more commonly known as “Let’s Encrypt”). Certificates signed by any other authority for official mirror FQDN shall be considered fraudulent. In the event of accidental generation, appropriate action(s) must be taken by all relevant parties to quickly invalidate, revoke, or otherwise disable the certificates. In the event that certificates cannot be disabled or revoked (ex. in the event of hostile takeover), TLS access to the mirror must be disabled and a notice posted in the information file.

Maintenance access

All PLUG users must utilize only the following methods to manage access mirror infrastructure:

- Hardware-backed SSH keys, utilizing an algorithm and keysize (if applicable) approved by all PLUG mirror maintainers. Hardware keys shall require an initialization pin and a per-use physical interaction (ex. a button push) prior to performing authentication. Any physical backups of hardware-backed keys must be stored in appropriately secured, offline storage mediums, which may never be connected to an internet-facing computer.

All RCAC users may only utiulize the following methods to access mirror infrastructure:

- RCAC bastion-host based access, using the well-known established key.

- Upon mutual agreement of a majority of maintainers, a temporary key for the purposes of maintaining mirror hardware.

If a user is both an RCAC user and a mirror maintainer, their access shall follow the PLUG user guidelines; they shall not, wherever possible, utilize bastion key(s).

In the event that a given user's account is breached (as determined at the discression of any mirror maintainer), the following actions must be taken:

- The user's access must be temporarily restricted (for a period not to exceed 5 days) by the first available maintainer
- The user must be notified
- Any relevant logging information pertaining to the user's actions must be saved indefinitely onto storage kept physically separate from the mirror itself

Any user (PLUG or RCAC) is subject to this key revocation policy.

Once the user has been notified, one of the following must occur in order for their access to remain restricted:

- The user agrees that a breach took place,
- A majority vote of the current maintainers must vote to keep the user's access restricted
- The user must be removed from the position of maintainer, or
- If they are a RCAC user, a mutually-agreeable solution is reached to prevent similar problems in the future

Information preservation & logging

Whenever practicable, any information which could be used to identify an end-user, to analyze their activities, or otherwise intrude on their privacy must be discarded.

To ensure the security and continuing stability of the PLUG mirror, the following instances shall be considered permissible for maintaining logs:

Data Type	**Example of data**	**Example medium**	**Time period**	**Notes**
Aggregate, anonymous data	Total goodput, number of TCP established sessions, number of visitors to the mirror overall, download totals	Time series database (ex. Prometheus)	Indefinitely	May be made public at the discretion of the maintainers.
Statistical, anonymous access data	Number of total visitors to a specific file within a given time period	Log parser output	Indefinitely	No more than 7 days information may be released publicly in a given month.

File access logs	Specific HTTP requests, specific FTP requests, specific RSYNC requests	NGINX access logs	1 week	Logs of a specific event may be preserved at the discretion of any maintainer for the purposes of an investigation.
Administrative logs	RSYNC requests to update the mirror	Internal sync logs of what we download when updating the mirror	2 weeks	May be maintained for a shorter period of time at the discretion of the maintainers.
Security logs	SSH authentication logs, bash/zsh/etc… command execution logs	Authentication log, command log	*Undisclosed*	Security logs which describe interaction outside of the supported protocols (ex. SSH) may be provided to RCAC and/or Purdue University at the discretion of the maintainers.

If logs are maintained for an investigation, the logs must be scoped to only contain information and context which is relevant to the ongoing investigation. If a valid court order is provided, this must contain the entire scope of the court order.

Security logs must be parsed, examined, and otherwise monitored for signs of intrusion. Log analysis may make use of third-party security tools. Security logs must not contain user-identifying information from HTTP, HTTPS, FTP, or RSYNC transfers.

At no point may user identifiable information from any non-security logs be made publicly available. Further, with the exception of publicly disclosed statistics, logging information from PLUG mirror must never be used for commercial purposes.

Public mirror information

Public disclosure of policies

In the interest of ensuring public trust in community-supported infrastructure, this document and all subsequent versions must be made publicly available on the PLUG mirror.

Information disclosure canary

Having been established in the interest of the broader public good, the following statements must appear on the mirror information page until such time that they may no longer be considered accurate:

- ‘We have not been asked by any law enforcement body/government agency to turn over logs, perform wiretaps, or to otherwise spy on individual users.’
- ‘We have not been subjected to mandatory key "escrow" of any sort, nor will we willingly do so.’
- ‘We are a US-based organization and are subject to US law and laws of the state of Indiana.’
- ‘Apart from mitigating abuse and as legally required, all do not track requests will be/are honored.’
- ‘Access to logs is only available to trusted PLUG mirror maintainers. A complete list of maintainers may be found above. We prohibit utilization of logs for purposes outside of those outlined above.’

Users with additional, non-standard access to the mirror

All users with access to the Purdue Linux Users Group mirror must be publicly known.

For PLUG mirror maintainers, the following information must be made publicly available:

- The maintainers preferred name
- A valid e-mail address for contacting the user (not necessarily a @purdue.edu e-mail address) and/or the user’s IRC and/or Matrix handle for any and all official PLUG chatrooms.

Additionally, the following note shall appear: “Additionally, RCAC personal have break-glass access to the mirror. Each instance of access of RCAC access to the mirror will be audited in accordance with PLUG policy.”

For projects with push-based access to the mirror, the following information must be made publicly available:

- The name of the project

Contact methods for Mirror Maintainers & RCAC personnel with access to the mirror

A mailing list shall be maintained which will copy messages to all mirror maintainers and RCAC personnel with additional, non-standard access to the mirror. Mailing list archives must be kept internal and shall not be shared publicly with members of the general public. Exceptions to this rule may be made in instances where the community interest outweighs the need for operational security, as determined by the PLUG mirror maintainers.

Internal mirror documentation

All users with additional, non-standard access to the mirror must be given access to an internal documentation repository. This repository shall contain up-to-date information describing mirror operations, common community contacts, policy implementations, and other relevant operations materials. Information in the internal documentation repository shall be treated as sensitive; while it may be shared externally at the discretion of the PLUG Mirror Maintainers, care should be taken to ensure that the information exposed does not risk the operational security of the mirror.