# Responsibilities and Processes for Website League Keyholders

*Also available at:*

*https://docs.google.com/document/d/1dn3gQ5BHvBDTwA6WJcdMq7dCy0rxkyuSck0ut2f1iJ4/view*

Last updated: 2024-12-13

## Rationale

To facilitate collaboration between Stewards, as well as to ensure all users have visibility into the workings of the Website League, the League operates a set of central, self-hosted services. The nature of these services requires a heightened level of trust in people that are given full administrative access to them, as a bad actor could use that access for a variety of malicious purposes (changing access permissions for various users, exfiltrating user data stored on central infrastructure such as emails, messages (both public and private), etc.).

In mitigating this risk, we introduce the concept of a “Keyholder” role. Keyholders are designated Stewards who have full administrative access to central infrastructure services, and are tasked with ensuring that infrastructure remains operational, secured, and up to date. The set of Keyholders should ideally remain limited to minimize the attack surface of central infrastructure, and Keyholder status should only be granted to people who can be trusted with its sensitive nature.

While Keyholders are trusted with access to more of the Website League’s infrastructure, this should not elevate them beyond the status of any other Steward in governance. The purpose of the Keyholder role is to ensure smooth operation of central League services, and to minimize the attack surface of those services by granting access to as few people as possible. Keyholders are not to be viewed as “above” Stewards in any sense, and Keyholders must not abuse their elevated access to attempt to subvert, disrupt, or overrule League governance processes.

## Current Keyholders

This list reflects the current state of who is granted Keyholder status. If, at any time, Keyholder status has been granted or revoked from any person, this section of the proposal is to be amended to reflect those changes.

The current list of people granted Keyholder status is as follows:

- srxl (Ruby)
- atomicthumbs
- sirocyl

# Audit Log

Any changes made to the list of Keyholders must be logged here, as an amendment to this proposal, for transparency.

- 2024-12-13 - srxl, atomicthumbs and sirocyl formalized as initial Keyholders

## Duties

Keyholders have a set of duties and expectations that they must follow as part of their role. These duties are as follows:

- Perform various system administration tasks on central League infrastructure as required. This includes, but is not limited to:
  - Configuring central services and ensuring they function as required by League members
  - Fixing any bugs/issues in central infrastructure identified by League members
  - Assigning/revoking roles that grant Stewards access to services needed to perform their duties
- Providing technical support for central infrastructure services to League members on a best-effort basis
  - This is not exclusively the domain of Keyholders - however sometimes a Keyholder is required to modify central infrastructure to fix an issue
  - Keyholders should, within reason, try to respond to support queries at their earliest convenience
- Perform regular maintenance on central infrastructure to keep services up to date
- Onboard new Keyholders, and offboard former Keyholders as Keyholder status is granted to/revoked from League members
- Send out announcements on the Buttondown newsletter and Broadcast as necessary
- Refrain from accessing any data stored on central infrastructure services, particularly user information or private messages, unless required to carry out any other Keyholder duties

# Processes

To ensure central infrastructure operates smoothly, and Keyholders remain aware of how to carry out their duties, there are a set of processes that Keyholders should follow.

- If changes are made to any central infrastructure, ensure that change is documented somewhere. This can include:
  - Bookstack

    - The “Infrastructure Operations” channel in Coordination
    - Consensus, if relevant to a discussion held there
- In the event of central infrastructure downtime (planned or unexpected), League members should be notified through at least one of the following channels, where available/necessary:
    - The Announcements channel in Coordination
    - Broadcast
    - The #announcements channel in the Website League Discord server
- If downtime is planned, an announcement should be made prior to the downtime occurring. The advance notice period is determined by Keyholders on a case-by-case basis, with longer downtimes requiring further advance notice.
- A regular update of all central Infrastructure services should be performed at least once every 3 months.
    - This should be conducted by one Keyholder, who is nominated to perform that specific update by all Keyholders.
    - Unless an update to a service would cause that service to stop working without significant work to mitigate the breakage, all services should be updated to their latest versions during these runs.
    - Any services that are not updated during a regular update should be logged with a ticket in Planning to ensure the update is eventually performed.
- To onboard a new Keyholder, the following tasks must be performed:
    - Create a new user on the central infrastructure VPS, and add an SSH key to that user
    - Add their Authentication account to the following groups:
        - Infrastructure Operators
        - Information Admins
    - Create a login with the requested username and password for Observation
    - Send out an invite to Vaultwarden and grant access to the credential vault
- To offboard a former Keyholder, the above tasks must be undone by removing accounts/keys as necessary.
- When a newsletter issue or a Broadcast announcement has been drafted, one Keyholder should be nominated to send out that announcement.

# Access

Keyholders require elevated permissions and access to various central infrastructure services to perform their duties. The additional access granted to Keyholders is as follows:

- Administrator (full) rights on the following services:
    - Coordination
    - Consensus
    - Broadcast
    - Information
    - Authentication
    - Planning
    - The website-league organization on GitLab
    - The Website League Discord server

- Individual accounts on the following services:
  - Observation
  - Vaultwarden
  - SSH to the central infrastructure VPS
- Credentials for the following accounts:
  - @league@websiteleague.org on Broadcast
  - Buttondown account for the newsletter
  - The infrastructure@websiteleague.org email inbox
  - The Google account managing our shared Google Drive
  - The SMTP service provider account
- Entry into the private “Infrastructure Operations” channel in Coordination

# Membership

Any Steward can be nominated to be a Keyholder through a proposal on Consensus. The process for nominating a Keyholder is the same as our process for nominating Stewards. Keep in mind that a very high level of trust is required for Keyholders, and as such, Keyholders should only be nominated if more Keyholders are desired, and if the nominee has demonstrated a high level of trustworthiness within the Website League already. Only existing Stewards are eligible to be nominated as Keyholders, to ensure that Keyholders are held accountable to the Stewardship body through the same mechanisms as all other Stewards.

At any time, a Keyholder may decide to temporarily relieve themselves of their duties for whatever reason, such as changes in personal circumstances leading them to be unable to adequately perform their duties as a Keyholder. In this event, access to all services listed under the Access section must be temporarily disabled, and a note is to be recorded in the Audit Log section of this document. At any time, they may choose to return to Keyholder duties, in which case an active Keyholder should re-enable all their Keyholder access and record another note in the Audit log.

Keyholders can also be removed from the role for the following reasons:

- If a Keyholder decides to voluntarily step down from their role, for whatever reason
- If a Keyholder has been inactive and unreachable in an official League capacity for at least 1 month
- If a Consensus vote is held to relieve a Keyholder from their duties for whatever reason, such as abuse of their elevated access or lack of trust by the community

---

Revision #1
Created 13 December 2024 01:09:01 by srxl
Updated 13 December 2024 01:16:28 by srxl