Terminating User Accounts from Your Enterprise

There are several termination/removal options available to your LastPass Administrator. Please consider your options carefully prior to deleting or removing users. These actions can be performed from the Users tab in the Admin Console using the Actions column, or can be automated using Directory Integrations. There are three main termination options:

- Disable User
- Remove User From Company
- Delete User

Disabling a user in your Enterprise puts a lock on the account. No one – not even your LastPass administrator – can log in to the account regardless of passwords or previous access. Once disabled, the license will be available for reassignment.

Removing a user from your Enterprise will disassociate (spin out) that user's account from your company account. With this action, all Shared Folder data will be revoked immediately. LastPass will also prompt if you would like to "Delete Shares" or "Do Not Delete Shares". Selecting to "Delete shares" will delete all sites within the account that have been shared to the user from other users in the Enterprise outside of Shared Folders. The account will otherwise still be fully available for use by this user, including all data that has been stored in the user's vault. Once removed, the license will be available for

reassignment.

Deleting an account **FULLY DELETES ALL CONTENTS** in the account. Any data stored within the account will be gone forever. Once deleted, the license will be available for reassignment.

Please note that all LastPass Enterprise licenses are transferable once an account is disabled, removed, or deleted.

Resetting a User's Master Password

This option is only available if the Super Admin – Password Reset policy is in place. From the Admin Console, the Admin of the Enterprise can reset the master password on the account. This option can be leveraged under the following scenarios:

(1) You would like to lock-out the owner of the account, but still allow Admin access. This can be helpful for audit purposes; in order to update and/or terminate any credentials to which the end user had access.

(2) If you would like to assign the entire account – with all of its contents – to another employee.

Important Considerations

- Ensuring that sites/tools are no longer accessible by the employee: If the account owner created any passwords in his vault, or if any credentials were shared visibly with him, then it is quite possible that he has stored this information elsewhere and could access these tools again in the future (outside of LastPass). In order to avoid any doubt, we therefore recommend updating all passwords when an employee account is terminated.
- Once terminated (disabled, deleted or removed), any data that the account owner has placed in a Shared Folder will remain fully intact for remaining users.
- In the case of Shared Folders, while you are never at risk of deleting the shared credentials, you are at risk of finding yourself with no remaining Admin on the folder (if the former account owner was the sole folder Admin). If this is a concern, you should consider enabling the 'Super Admin – Shared Folders' policy.
- **NONE** of these actions will affect a Linked Personal Account, which is why we **HIGHLY RECOMMEND** users utilize the Linked Personal Account Tool rather than storing personal data in an Enterprise account.