

# Families-as-a-Benefit Policies

## CHALLENGE

The popular LastPass Families-as-a-Benefit option, which is enabled by default, gives each business user five complimentary licenses to share with family and friends – helping to spread the security benefits. As well as giving friends and family members their own personal password vaults, it allows employees to set up a personal vault, alongside their work vault. Users can simply drag and drop passwords and login credentials from one vault to the other.

While this is convenient for users, businesses may be concerned about the risk of confidential business data being moved into an employee's personal password vault – either accidentally or deliberately.

## SOLUTION

To minimize the risk of confidential business information finding its way into personal accounts, LastPass offers some useful policies that allow your managed service provider (MSP) or administrator to set rules about how and where passwords are stored, and how they can be moved.

## HOW IT WORKS

There are essentially three policies that can be implemented to minimize the risks of confidential data being shared as a result of the Families-as-a-Benefit feature. These policies can be applied to the whole business, or to specific groups or individuals:

### 1. Prohibit Families-as-a-Benefit

This is the strictest measure. It simply prohibits the user from claiming the free LastPass families account to manage their personal passwords.

### 2. Prohibit update of personal account information

This policy restricts users' ability to add, update, or delete data in a linked personal account, when they are logged in to their LastPass business account. Essentially, it prevents employees from being able to drag and drop content from their business vault into their personal vault.

### 3. Save personal sites to personal vault

When this policy is enabled, sites with a username matching the user's linked personal account are saved directly to the personal vault only. Sites with any other username are saved to the user's business vault.

NOTE: To protect the security of employees and their families, none of the data or passwords stored within their personal accounts can be accessed by the employer. Your LastPass administrator or MSP can only see whether a user has claimed their LastPass Families-as-a-Benefit account. Any personal account information or passwords stored in the personal vaults remain private, and are only visible to the individual user.

## OUTCOME

By setting rules for the use of personal LastPass accounts and their connection to business accounts, you can prevent employees from accidentally or deliberately sharing confidential business passwords and data outside your organization.

The policy rules are controlled centrally. They can be applied to the whole company, specific groups or individual users, according to your business requirements. It's another way in which LastPass helps to secure your business and its data against cybersecurity risks.

**To find out more about benefits of LastPass and the Families-as-a-Benefit feature, please contact your MSP.**