What you can do

# What you can do#

It's also your responsibility as a customer to ensure you are securing your code and data. This document lists some steps you can take.

## All users#

• Report security issues and terms of service violations to security@n8n.io.

• If more than one person uses your n8n instance, set up User management and follow the Best practices.

• Use OAuth to connect integrations whenever possible.

## Self-hosted users#

If you self-host n8n, there are additional steps you can take:

• Set up a reverse proxy to handle TLS, ensuring data is encrypted in transit.

• Ensure data is encrypted at rest by using encrypted partitions, or encryption at the hardware level, and ensuring n8n and its database is written to that location.

• Run a Security audit.

• Be aware of the Risks when installing community nodes, or choose to disable them.

• Make sure users can't import external modules in the Code node. Refer to Environment variables | Nodes for more information.

• Choose to exclude certain nodes. For example, you can disable nodes like Execute Command or SSH. Refer to Environment variables | Nodes for more information.

• For maximum privacy, you can Isolate n8n.

### GDPR for self-hosted users#

If you self-host n8n, you are responsible for deleting user data. If you need to delete data on behalf of one of your users, you can delete the respective execution. n8n recommends configuring n8n to prune execution data automatically every few days to avoid effortful GDPR request handling as much as possible. Configure this using the EXECUTIONS\_DATA\_MAX\_AGE environment variable. Refer to Environment variables for more information.

EXECUTIONS\_DATA\_MAX\_AGE