



## Cloud Shared Responsibility Guide

---

**Purpose**

Nobly provides secure cloud-based services built on Microsoft Azure. Maintaining the security of our services is a shared responsibility between Microsoft, Nobly and our customers.

This guide explains those responsibilities and helps customers understand how security is managed throughout the service lifecycle.

The responsibilities described here complement, but do not replace, the contractual obligations defined in applicable Data Processing Agreements or Service Agreements.

**Scope**

This guide applies to Nobly-hosted SaaS services operated in Microsoft Azure.

It describes the shared security responsibilities for the cloud services operated by Nobly. It does not apply to customer-managed infrastructure, third-party services, customer integrations, or on-premises deployments unless explicitly agreed.

**Shared responsibility model**

Cloud security is based on a shared responsibility model involving three parties:

| Party     | Responsibility                                                                                                                                               |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft | Secures the Azure cloud infrastructure, including physical data centres, networking, virtualisation and core cloud services.                                 |
| Nobly     | Develops, operates and secures the Nobly cloud services, including the application, supporting infrastructure, monitoring and operational security controls. |
| Customer  | Securely uses the Nobly service by managing users, permissions, uploaded data and internal governance processes.                                             |

**Security responsibilities**

| Security area                  | Microsoft | Nobly | Customer |
|--------------------------------|-----------|-------|----------|
| Physical security              | ✓         |       |          |
| Azure cloud infrastructure     | ✓         |       |          |
| Application security           |           | ✓     |          |
| Secure software development    |           | ✓     |          |
| Vulnerability management       | ✓         | ✓     |          |
| Security monitoring            | ✓         | ✓     |          |
| Service backups                |           | ✓     |          |
| Disaster recovery              | ✓         | ✓     |          |
| Identity and access management | ✓         | ✓     | ✓        |
| Customer user administration   |           |       | ✓        |
| Customer data management       |           | ✓     | ✓        |
| Incident management            | ✓         | ✓     | ✓        |

Responsibilities may involve more than one party where each party is responsible for different aspects of the same security area. The sections below describe these responsibilities in further detail.

**Detailed responsibility****Identity and access management**

Nobly:

- Protects administrative access through role-based access control.
- Uses phishing-resistant authentication for privileged access.
- Uses Just-in-Time (JIT) privileged access to minimise standing administrative privileges.
- Performs regular access reviews.
- Removes employee access promptly when no longer required.

Customer:

- Creates, manages and removes customer user accounts.
- Assigns user permissions appropriate to business needs.

- Protects user credentials.
- Enables Multi-Factor Authentication (MFA) or phishing-resistant authentication where available and appropriate.
- Reviews user access regularly.

## **Data protection**

Nobly:

- Processes personal data only on documented customer instructions.
- Implements appropriate technical and organisational security measures.
- Encrypts customer data in transit and at rest.
- Maintains secure backups and recovery capabilities.
- Assists customers in fulfilling applicable processor obligations under the Data Processing Agreement.
- Notifies customers without undue delay if a personal data breach affecting their data is identified.

Customer:

- Determines the purposes and legal basis for processing personal data.
- Decides which information is uploaded to the service.
- Classifies information according to its own policies.
- Manages the retention and deletion of data stored within the service.

## **Service security**

Nobly:

- Develops and maintains the application using secure development practices.
- Performs vulnerability management and security testing.
- Operates continuous security monitoring and logging.
- Maintains incident response, business continuity and disaster recovery capabilities.
- Performs regular backups of the service.
- Operates a formal change management process, including security and risk assessment for changes that may affect the service.

Customer:

- Reports suspected security incidents affecting its users or environment.
- Maintains accurate administrative contact information.
- Notifies Nobly if customer accounts are believed to be compromised.

- Uses the service in accordance with Nobly's terms and security guidance.

## **Frequently asked questions**

### **Does Nobly manage our users?**

Customers are responsible for creating, modifying, and removing their own users unless otherwise agreed.

### **Does Nobly classify our data?**

Customers determine the classification and sensitivity of the information uploaded to the service.

### **Can Nobly delete our data?**

Customers remain in control of the data they upload to the service and are responsible for managing the retention and deletion of data stored within the service.

Nobly does not monitor, select, or delete data as part of normal service operations. Upon termination of the service, any remaining customer data is deleted by Nobly in accordance with the applicable contractual terms and Data Processing Agreement.

### **Who is responsible if a user's credentials is compromised?**

Nobly secures the platform and administrative accounts under its control. Customers remain responsible for protecting their own user credentials and following their internal security policies.

### **Does Nobly perform backups?**

Nobly performs backups of the service to support service resilience and disaster recovery. Customers remain responsible for ensuring that the service meets any internal legal, regulatory or business requirements relating to data retention or data export.

### **Who reports GDPR breaches?**

If Nobly becomes aware of a personal data breach affecting customer data, Nobly will notify the customer in accordance with the Data Processing Agreement.

The customer, as data controller, determines whether notification to supervisory authorities or data subjects are required.

**How does Nobly secure its cloud environment?**

Nobly maintains an information security management system aligned with ISO 27001 and undergoes annual independent ISAE 3000 type II assurance.

Security measures include:

- Secure software development lifecycle
- Phishing-resistant authentication
- Just-in-time privileged access
- Security monitoring and logging
- Vulnerability management
- Regular penetration testing
- Business continuity and disaster recovery planning
- Risk-based change management
- Annual independent assurance

**Related documents**

For further information, please refer to:

- External information security policy
- Data Processing Agreement
- Privacy Policy
- ISAE 3000 Type II assurance report (available upon request)