Our Security Measures

Learn how we keep your data secure

At Goldphish, we are committed to protecting the confidentiality, integrity, and availability of our information systems and our customers' data. We continuously improve our security controls and analyse their effectiveness to ensure confidence in our solution.

Below is an overview of some of the security controls in place to protect your data.

Data Center Physical Security

FACILITIES

Goldphish uses IONOS for data center hosting. IONOS data centers are certified as ISO 27001 compliant by the Technical Inspection Association (TÜV). They employ robust controls to secure the availability and security of their systems, including backup power, fire detection, suppression equipment, and secure device destruction.

ON-SITE SECURITY

IONOS implements layered physical security controls, including vetted security guards, fencing, video monitoring, intrusion detection technology, and more.

Network Security

THREAT DETECTION

Goldphish leverages threat detection services within IONOS to continuously monitor for malicious and unauthorised activity.

VULNERABILITY SCANNING

We perform regular internal scans for vulnerabilities. Identified issues are tracked until remediation.

DDOS MITIGATION

Goldphish uses multiple DDoS protection strategies and tools to mitigate threats. We utilise IONOS's DDoS protection and application-specific mitigation techniques.

ACCESS CONTROL

Access is limited to the least privileged model required for staff. This is subject to frequent internal audits, technical enforcement, and monitoring to ensure compliance. Multi-factor authentication (MFA) is required for all production systems.

Encryption

IN TRANSIT

Communication with Goldphish is encrypted with TLS 1.2 or higher over public networks. We adopt best practices in terms of cipher adoption and TLS configuration.

AT REST

Goldphish data is encrypted at rest with industry-standard AES-256 encryption. By default, we encrypt at the asset or object level.

CREDENTIALS ENCRYPTION

Credentials for the production database are regularly rotated to ensure access restriction.

Availability & Continuity

UPTIME

Goldphish is deployed on public cloud infrastructure. IONOS offers close to 100% availability with multiple redundant connections to major Internet hubs. Our services are deployed to multiple availability zones for availability and are configured to scale dynamically in response to load. Simulated load tests and API response time tests are part of our release and testing cycle.

DISASTER RECOVERY

Our services are deployed in parallel at two separate data centres. In the event of a problem at one data centre, the system automatically switches to the second, ensuring continuous availability.

DATABASE RECOVERY

Our database has point-in-time recovery for up to four days and is manually backed up daily, with a maximum of 30 backups.

UPS POWER SUPPLY

IONOS data centres maintain an uninterruptible power supply (UPS) due to emergency diesel generators and VRLA batteries.

Application Security

QUALITY ASSURANCE

Goldphish's Quality Assurance team reviews and tests code per pod basis. The security team investigates and recommends remediation of security vulnerabilities within code.

ENVIRONMENT SEGREGATION

Testing, staging, and production environments are logically separated. No customer data is used in any development or test environment.

APPLICATION SCANNING

Site Scan from SiteLock is used to protect our site from hackers, malware, and unauthorised access.

PENETRATION TESTING

We carry out annual penetration tests to identify and address potential security vulnerabilities. These tests are performed by independent security experts to ensure the highest level of security for our systems and data.

Endpoint Security

ANTI-VIRUS

We implement endpoint Antivirus and run daily scans on our machines.

PASSWORD POLICY

Goldphish enforces a strong password policy across all servers, systems, and devices, in conjunction with mandatory multi-factor authentication on all production and business systems. Passwords are never shared or reused across systems, and are stored using industry-standard encryption.

SPAM CHECKS

All incoming emails are filtered for SPAM and quarantined for checking before delivery to the network.

REMOTE WORKING

Goldphish operates a 100% remote working international team. Staff are not permitted to work on personal computers unless prior agreement has been stated.

CYBER ESSENTIALS ACCREDITED

Goldphish is Cyber Essentials certified, demonstrating our commitment to maintaining robust cybersecurity standards and protecting against common cyber threats.

Verify our current certification status on the IASME Certificate Search under 'Goldphish Ltd'.

Personal Security

SECURITY AWARENESS

Goldphish delivers a robust Security Awareness Training programme within 30 days of new hires and continuously for all employees. Quarterly focused training is rolled out to key departments, including Secure Coding, Data Legislation, and Compliance obligations.

INFORMATION SECURITY PROGRAMME

Goldphish has a comprehensive set of information security policies covering various topics. These are disseminated to all employees and contractors, with acknowledgement tracked on key policies such as Acceptable Use, Information Security Policy, and our Employee Handbook.

EMPLOYEE BACKGROUND CHECKS

All Goldphish employees undergo a background check covering 5 years criminal history (where legal) and 5 years employment verification before employment.

CONFIDENTIALITY AGREEMENTS

All employees are required to sign Non-Disclosure and Confidentiality agreements.

ACCESS CONTROLS

Access to systems and network devices is based on a documented, approved request process. Logical access to platform servers and management systems requires two-factor authentication. Access is further restricted by system permissions using a least privilege methodology. Business need revalidation is performed quarterly to ensure access is commensurate with the users' job function. User access is revoked upon termination of employment or change of job role.

Third-Party Security

VENDOR MANAGEMENT

Goldphish understands the risks associated with improper vendor management. We evaluate and perform due diligence on all of our vendors before engagement to ensure their security is to a suitable standard. If they do not meet our requirements, we do not move forward with them. Selected vendors are then monitored and reassessed on an ongoing basis, considering relevant changes.

Data Privacy

Here is some key information on how we securely store your data.

Supplier name	**Company Number**	**ICO Number**
Goldphish Ltd	10333752	ZA276913

Sub-processors	**Data Protection Lead**
(used to process personal data) - IONOS - Hubspot - Wix - MailGun - Google - Xero - Stripe - HelpScout	These responsibilities are shared between Dan Thornton (CEO) and Marius Potgieter.

WHAT WE'RE STORING

We store only necessary information, as collected by you. We never store any of your users' credentials that are compromised during a phishing simulation. Our phishing simulation landing pages do not capture data entered on the phishing landing pages; it only tracks that the user failed the data entry portion of the test.

HOW WE'RE STORING IT

We encrypt your data both at rest and in transit. Our site and storage processes are designed for security.

WHO CAN ACCESS IT

We have extensive internal access controls and regulations for the Goldphish team, who only have access to data under limited conditions. You can restrict admin access to sensitive materials.

OUR CORE STANDARDS

Our core compliance with the act means that:

- We maintain full awareness of where your data is being held, ensuring appropriate compliance outside of the UK.
- We ensure that only those who require access to your data can access it and have the highest level of protection against unauthorised access.
- We ensure you have the right to view, amend, export, or delete any information that we hold on your behalf, including anything held by 3rd party services.
- We ensure that consent is given during the signup process for all that use Goldphish and allow you to withdraw at any time.

PRIVACY POLICY

Goldphish's privacy policy, which describes how we handle data input into Goldphish, can be found at **Privacy Policy**. For privacy questions or concerns, please contact info@goldphish.com.

For details on our incident response commitments and breach notification timelines, please refer to your Service Level Agreement or Data Processing Agreement.

Identifying, accessing, and amending data	**Deleting data from the application**	**Downloading user information**
Customers have the ability to identify, access, and amend their own data within the Goldphish platform which can only be accessed by authorised individuals in the business.	Data can be deleted from the application by the customer and restored within 7 days, at which point it is removed from the Goldphish database permanently.	Customers can also download the user information out of the application for use within their own reporting tool.

Last Updated: **9 July 2026**