DRAWBOARD

Drawboard’s approach to security

Drawboard’s mission is to increase productivity and reduce paperwork. We take the security of your data seriously and do the utmost to ensure that you are protected. We’re committed to being transparent about our security practices now and in the future.

Drawboard is developing its security program to align with ISO27001 standards and will continue to enhance existing measures into the future.

Personnel Security

- All company devices in the organisation are inventorised and tracked.
- All software platforms used in the organisation are inventorised.
- Drawboard's position in the market is clearly communicated with employees.
- Drawboard's place in critical infrastructure and the industry sector is identified and communicated with employees, we know how important your data is.
- Access permissions to all company's resources are managed, incorporating the principles of least privilege and separation of duties.
- Privileged users understand their roles and responsibilities.
- Access into the Drawboard's offices is controlled by an electronic key card access system.
- Employees follow a strict on boarding and off boarding process when entering and exiting the company. When an employee has exited the company, all access is revoked.
- Drawboard's internal network is routinely monitored for unknown connections.

Physical Security

Drawboard stores your data in the Microsoft Azure cloud, an industry leader in hosted facility management.

- Access to Microsoft data centres requires multi factor authentication and all access is logged. Data centre access logs are routinely monitored.
- Highly trained security personnel are present at data centres 24/7.
- Uninterrupted power supply prevents any downtime with backup generators installed in every data centre.

For more information please visit https://www.microsoft.com/en-us/trustcenter/security

Infrastructure Security

- Access to customer data is limited and only provided when prior consent has been granted by the customer.
- Code repositories are locked down using 2 factor authentication.
- Code repositories are locked down and all changes are transacted using Pull Requests which provide a full audit trail of all changes made.
- IP addresses are locked down so only critical personnel have remote desktop access (RDP) into Windows Azure using network Access Control Lists (ACL) to ensure only known networks can get access to VMs.
- Access to Windows Azure is locked down incorporating the principles of least privilege and separation of duties.
- Document uploads are scanned prior to their acceptance and are limited to only supported file types.
- Drawboard Development, Test and Production and Customer Enterprise environments are independent of one another.
- Hosted machines are routinely patched and maintained as part of the Microsoft Azure Cloud.

Application Security

- Data is encrypted both in transit (TLS – 2048 bit – using LetsEncrypt CA) and at rest (Azure Storage-wide encryption using AES256).
- User passwords are salted and hashed (using PBKDF2 algorithm with 25 000 iterations) and in the future, will be stored in Auth0 or Clients Active Directory federated with our service.
- Third party “secret” data is always kept independent of the code.
- Drawboard’s API uses the industry standard Open ID Connect (OIDC) authorisation protocol.
- Drawboard’s API traffic is monitored and triggers alerts when abnormal use occurs.

- Single Sign On (SSO) is currently in development which will allow integration with Azure Active Directory (AAD).
- Application access is permission based with four access levels (Owner, Admin, Collaborator and Reader). Permissions are checked when data is accessed in the platform.

Compliance

- Drawboard applications are tested by industry leading vendors.
- Drawboard provides tooling to allow customers to export their data in full from the platform ensuring that data is not locked down and can be removed at any time.
- Drawboard does not store any PCI-related payment information on its servers and Drawboard employees have no access to payment information.
- For enterprise agreements at the customer's request event tracking for marketing purposes will be disabled.