iPages Information Security Policy

The purpose of the iPages Information Security Policy is to set the objectives for information security management to preserve our commitment to our customers. This is the overarching policy that explains the key ways that iPages ensures the secure handling of its information while providing appropriate access.
This includes setting policies in the following areas:

- iPages' Data Protection
- Data Protection where iPages is the Data Processor
- Access Control
- HR Security
- Security Scans

iPages uses the best practices described in the ISO 27002 security standard. This standard is recognized globally as the most comprehensive framework for establishing and maintaining information security best practices within an organization. As these controls are essential to our security posture, we refrain from describing them in detail on publicly available documents however; we do describe how these best practices are met.
Additional security policies related to physical asset management are defined within the End User Device Security Policy.

1. DATA PROTECTION

1.1. iPages is a registered with the ICO (ZA550728) under the Data Protection (Charges and Information) Regulations 2018.
1.2. iPages meet their GDPR obligations through:
1.2.1. keep data personal data secure through secure hosting and documented Information Security Polices;
1.2.2. when a personal data breach is suspected, iPages shall,
1.2.2.1. notify the ICO within 72 hours;
1.2.2.2. notify the affected data subjects and;
1.2.2.3. keep a record of all instanced of notifying the ICO.

2. DATA PROTECTION WHERE KHOO SYSTEMS IS THE DATA PROCESSOR

2.1. As per our Terms and Conditions, relating to Customer data or data held with a Customer's instance of the software, iPages are therefore appointed as a Data Processor and the Customer is the Data Controller.
2.2. The Data Controller has overall control of personal data held within a iPages provided system
2.3. A Customer's Proposal will state the Customer and Khoo System's contract term and, for the purposes of data protection, this same term shall apply.
2.4. We may only process personal data in line with the controller's documented instructions (including when making an international transfer of personal data) unless it is required to do otherwise by EU or member state law
2.5. We must obtain a commitment of confidentiality from anyone it allows to process the personal data, unless that person is already under such a duty by statute.
2.6. iPages have put in place appropriate technical and organisational measures to ensure the security of any personal data we process which may include, as appropriate:
2.6.1. encryption and pseudonymisation;
2.6.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
2.6.3. the ability to restore access to personal data in the event of an incident; and
2.6.4. processes for regularly testing and assessing the effectiveness of the measures.
2.7. iPages will not engage another processor (a sub-processor) without the controller's prior specific or general written authorisation.
2.8. iPages supports it's Customer's in meeting their GDPR obligations through:
2.8.1. keep data personal data secure through secure hosting and documented Information Security Polices;
2.8.2. when a personal data breach is suspected, iPages shall, with the Customer:
2.8.2.1. notify the ICO within 72 hours;
2.8.2.2. notify the affected data subjects and;
2.8.2.3. keep a record of all instanced of notifying the ICO.
2.9. Upon termination of an Agreement, iPages shall, at the end of the Service provision;
2.9.1. delete or allow the Customer to extract all the personal data from the hosted software platform;
2.9.2. delete existing copies of the personal data unless EU or Member State law requires it to be stored, for example for invoice records.
2.10. Should the Customer appoint an auditor to audit the Customer's use of data, iPages shall allow for this audit.

3. ACCESS CONTROL

iPages dictate the following around their internal staff access to software, networks, and information, according to the staff member's role:
3.1. Generic or test IDs must not be created or enabled on production software, networks or Customer accounts unless specifically authorized by the Information Security Officer.
3.2. Passwords or pass phrases must be lengthy and complex, consisting of a mix of letters, numerals and special characters that would be difficult to guess.
3.3. Passwords or pass phrases must not be written down or stored in readable format. iPages uses 1Password as the encrypted application for password storage for staff.
3.4. Privileged access rights typically required to administer, configure, manage, secure and monitor IT systems must be reviewed periodically (at least twice a year) by Information Security and cross-checked by the appropriate departmental managers.
3.5. Users must either log off or password-lock sessions before leaving them unattended.
3.6. Password-protected screensavers with an inactivity timeout of no more than 10 minutes must be enabled on all workstations.
3.7. iPages, as per our End User Device Policy, permits no use of USB drives or CD/DVDs for data transfer.

4. HR SECURITY

iPages mandates that:
4.1. All employees must be screened prior to employment, including identity verification using a passport or similar photo ID and, if deemed necessary by iPages, two satisfactory professional references.
4.2. All employees, within must formally accept a binding confidentiality or non-disclosure agreement concerning personal and proprietary information provided to or generated by them in the course of employment.
4.3. An employee must ensure that all devices are returned by the employee on or before their last day of employment.

5. SECURITY VULNERABILITY

In relation to the Services provided:
5.1. iPages shall maintain the necessary compliance for the Services provided:
5.1.1. Quarterly PCI DSS compliance vulnerability scans with a resultant compliance certification and vulnerability report.