Data security commitment

At Hornbill, safeguarding the confidentiality, integrity, and availability of information is paramount. Our commitment to data security is exemplified by our certification to the ISO/IEC 27001:2022 standard, which underscores our dedication to implementing and maintaining a robust Information Security Management System (ISMS).

Leadership and commitment

Our senior management demonstrates unwavering support for our ISMS by:

- Establishing and maintaining an information security policy aligned with our strategic objectives.
- Integrating information security into organizational processes.
- Allocating necessary resources to support the ISMS.
- Promoting a culture of continual improvement in information security practices.

Risk management and control implementation

We conduct regular risk assessments to identify and address potential threats to our information assets. Based on these assessments, we implement appropriate controls from ISO/IEC 27001:2022 Annex A to mitigate identified risks effectively.

Continuous improvement and monitoring

Hornbill is committed to the ongoing enhancement of our ISMS. We achieve this through:

- Regular internal audits and management reviews to assess ISMS performance.

- Monitoring and measuring information security objectives.
- Implementing corrective and preventive actions to address nonconformities.

Stakeholder engagement and communication

We recognize the importance of transparent communication with our stakeholders. Hornbill ensures that information security policies and procedures are communicated to all relevant parties, including employees, contractors, and clients, fostering a shared responsibility for data protection.

Our data security commitments

Below are some of the key points:

- All data transmitted from Hornbill network will be encrypted.
- All data is stored within the legal geographical entity associated with your head office (unless requested otherwise).
- Hornbill will not use any of your data for marketing or advertising unless specifically agreed with yourself (for example, in a case study).
- Hornbill will not access any of your instance data unless you specifically provide authorization (for example in the case of a support query). We will treat your data like a black box.
- Any request by 3rd party to access your data will be submitted to yourselves for approval before any action is taken.
- Any change to the existing sub-contractors (https://wiki.hornbill.com/index.php/FAQ:Subprocessors) will be disclosed to yourselves prior to change.
- Hornbill is committed to achieving all compliance with all applicable laws governing data in your geographical location. This includes GDPR, Data Protection Act, HIPAA.
- Any processing of log files for analytics will be anonymized.
- We will inform you within 24 hours of any suspected data breach.
- We will report any malicious activity on the services we provide, should the need arise. For example, low level "background" threats such as port scans that may occur will not be reported. However, a sustained attack against a specific instance or end point may be reported, even if the attack is not successful.

Trust and security is a two-way path and to this end we request that you meet the following:

- Always use strong passwords to secure your instance.
- Always use the encrypted protocols when given the change (POP3s, SMPTS, etc).
- Inform us within 24 hours if you suspect accounts linked to Hornbill have been breached.

Any questions or concerns can be raised via data.processor@hornbill.com. For more information about our data security practices or to request details about our ISO/IEC 27001:2022 certification, please contact our Information Security team at security@hornbill.com.