Data Security Commitment

Hornbills' commitment to data security and confidentiality is paramount in everything we do. To this end we have undertaken several objectives (including ISO27001 and 27018) to ensure your data remains secure at all times.

The pages within the wiki and your contract agreements detail how we do this in detail, however, below are 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\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 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 etc that may occur will not be reported, however a sustained attack against a specific instance or end point may, even if not successful).
- Any questions or concerns can be raised via data.processor@live.hornbill.com

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.

Hornbill believes in being open and we provide our documentation\policies and procedures at https://wiki.hornbill.com/FAQ:ISO/ for all. However, Enterprise customers can schedule a full-on site review of all polices should they wish and if required you should contact your account manager.