Cybersecurity Policy

Cybersecurity Statement

At HATS, a commitment to cybersecurity in the workplace is part of our approach to doing business. We commit to taking measures to protect against the criminal or unauthorised use of electronic data.

Cybersecurity Commitments

At HATS we ensure the protection of electronic data. To achieve this, we commit to:

- providing, maintaining and using secure electronic data systems
- providing methods for safely working with electronic data
- providing any information or training needed for our personnel
- monitoring the performance of our cybersecurity

Responsibility

HATS considers all HATS personnel as responsible parties in meeting the commitments stated in this policy. Ultimate responsibility of this policy and any supporting documents and procedures lie with the Directors of HATS.

All HATS personnel are obligated to understand this policy, the stated commitments and their responsibility to meeting these commitments.

All HATS personnel are to adhere to the following:

- Be wary of impersonation emails and phone calls and confirm identification before acting.
- Use MS Teams for internal communication unless otherwise agreed.
- Only use the systems provided by HATS for the storage of data (e.g. SharePoint) and do not store data on personal devices.
- Use multi-factor authentication where possible.
- Do not access external websites through hyperlinks provided in unverified communication.
- Payable invoice payments are to be actioned only by the Office Manager, who is responsible for confirming the bank details provided. Any request for invoice payment must be received by MS Teams or in person.
- Do not use unsecured internet networks.

DIRECTORS SIGNATURES 1 June 2024

Ryan Singh

Jiri Herza

James Thorp