



Halstead Town Council

Policy on intangible risks

Ensuring the on-going effectiveness of risk management requires strong and sustained commitment by the leaders of the organisation as well as strategic and rigorous planning to achieve commitment at all levels. The tone set by senior management towards risk management has the greatest impact on organisational appetite for risk. Risk appetite is best summarised as “the amount of risk an organisation is willing to accept” and is about looking at both the propensity to take risk and the propensity to exercise control. Halstead Town Council aims to be risk aware, but not overly risk averse and to actively manage business risks to protect and grow the organisation. To deliver its corporate priorities, the organisation recognises that it will have to manage certain business risks. **It maintains reviews and updates of risks facing the organisation and how they are being mitigated and ensures that these are visible at the highest levels in the organisation.**

Intolerable risks are those that could:

- ☐ Negatively affect the safety of employees or our customers/clients
- ☐ Have a damaging impact on our reputation
- ☐ Lead to breaches of laws and regulations
- ☐ Endanger the future operations of the council.

Culture, strategy and competitive position all influence our risk appetite and defining it forces the debate and ensures our risks are made explicit.

Safety

HTC seeks to minimise the physical risk to employees, councillors and clients. Any physical risk to which someone is exposed also represents a potential risk to the reputation of the council.

Reputation

HTC expects all employees and councillors to behave in such a way as to minimise risk to the reputation of the council, which has been built up over many years. Activities which may attract risk to reputation include idle talk, gossip, communication on social media about council matters, talking to the press on council matters, failure to adhere to the council's policy on the press and media.

Breaches of law and regulation

Council employees and councillors must at all times be seen to comply with those laws and regulations which govern the management of town councils, such as standing orders, financial regulations, code of conduct, good governance and robust financial management. Any breach of these would severely damage the reputation and future credibility of the council.

Risks to future operations of the council

Employees and councillors must ensure that they do not put the council's reputation at risk through any foolish act, reckless management of money, or decision lacking in judgement which may jeopardise the whole future of the council. Loss of data, business interruption through natural disaster or cyber attack are all events for which the Council must be prepared and vigilant.

Data protection and back-up

HTC data is backed up every night at 19.00 Mon-Sun. **Onsite** is deployed in fully secure and redundant data centres that are certified for SOC-2, ISO 27001, and PCI-DSS.

With regards to security:

Physical Security:

The datacentre is staffed 24/7/365 with onsite security and to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacentre internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Each facility is unmarked so as not to draw any additional attention from the outside, and adheres to strict local and federal government standards.

Storage Data Security:

Onsite is secure by default and all data stored in the **Onsite** cloud is always encrypted at rest (even if the requesting party doesn't specify encryption). **Onsite** follows industry-best security models and security design practices. Examples of **Onsite** security features include:

- HTTPS is supported for the secure upload/download of data
- Buckets are only accessible to the bucket and object creators
- **Onsite** supports user authentication to control access to data (including support for the AWS IAM model)
- Access control mechanisms such as bucket policies and Access Control Lists (ACLs) can be used to selectively grant permissions to users and groups of users

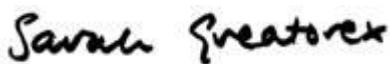
The link below which provides in-depth information on the specific data centre in California that holds HTC information and the company that operates it.

<https://www.ironmountain.com/digital-transformation/data-centers/locations/virginia-data-center>

Decisions taken by the council are taken collectively and all, employees and councillors, must take collective responsibility.

Sarah Greatorex Town Clerk Reviewed August 23

Recommendation: that HTC approves the update to the Policy on intangible risk



Sarah Greatorex Town Clerk