Information Security Policy

November 2023

Statement from the Executive Team

“As the world’s leading open hotel commerce platform, technology is essential to the consistent delivery of a positive customer experience.”

Technology remains at the forefront of the SiteMinder strategy. Our platform enables hotels to streamline their day-to-day operations, giving flexible pathways to start, upgrade or scale their business through the largest ecosystem of best-in-class hotel technology integration, application, and partners.

Good security underpins our intensive reliance on technology. While technology allows us to service our customers with utmost efficiency, it exposes us to additional security risks. SiteMinder must be committed to ensuring the safety and security of the data of its stakeholders, including its customers, partners, and employees.

To safeguard against information security events, we have developed a robust security policy framework that outlines the measures implemented to ensure we adhere to best practice, and comply with our regulatory obligations, including the EU General Data Protection Regulation (GDPR) and the Australian Privacy Act (1988). We have also aligned this framework with the Payment Card Industry Data Security Standards (PCI DSS) and ISO27001, an international standard on information security.

It is essential that we work together as a team to uphold the security measures in the policy framework. We encourage staff to take accountability and initiative in securing the information that was entrusted to us by our customers.

Information Security Principles

SiteMinder has five key information security principles that set out the high-level expectations, behaviours and values of our business and our staff when protecting our information. These principles are supported in our information security standards, which contain the detailed security requirements to keep our systems and data safe.

These key principles are as follows:

1. We must take a risk management approach to information security.
2. Our staff are our most important defence against security threats.
3. We safeguard access to protected information.
4. We apply safeguards to protect our information.
5. We comply with our legal and regulatory obligations.

These principles are further discussed below:

1. We must take a risk management approach to information security.

Taking a risk management approach to information security is essential in ensuring that our resources and attention are focussed on the areas that pose the greatest security risks to SiteMinder, which must be balanced against our business requirements.

SiteMinder must:

- Ensure that information security risks are managed within our risk appetite
- Conduct information security risk assessments
- Communicate identified risks with key stakeholders

2. Our staff are our most important defence against security threats.

Our staff are our first and most important line of defence against security threats. Individual accountability of cybersecurity practices are part of the culture of SiteMinder. Employees have acknowledged and understood their part in safeguarding our information.

SiteMinder must:

- Foster a culture of security awareness
- Ensure that information security obligations, policies and procedures are communicated to all staff
- Understand individual accountabilities and commit to information security practices
- Train staff on how to best manage information security risks

3. We safeguard access to protected information.

We classify our information according to its sensitivity and business impact. We ensure that restricted data is accessible only to people who are authorised to access the information.

SiteMinder must:

- Ensure that access is limited to what is necessary to perform the user's intended role or function
- Regularly review and monitor access to information
- Classify information

4. We apply safeguards to secure our information.

By adopting the industry best practice, we ensure that the appropriate technical, administrative, and physical safeguards are used to secure our information.

SiteMinder must:

- Comply with the information security framework
- Review the policy and associated standard to ensure that the documents are fit for purpose
- Manage exceptions to the standards and ensure each one is assessed for risks
- Continually improve the suitability, adequacy, and effectiveness of the information security management system

5. We comply with our legal and regulatory obligations

We are on top of all relevant legal and regulatory obligations on information security.

SiteMinder must:

- Document and regularly review relevant laws and regulations
- Monitor legal and regulatory compliance

Document Details

Authorisation

This document has been authorised and approved by:

Name	Authority	Date
Sankar Narayan	CEO	October 2022
Michael Tuton	Director of Security	August 2022

Revision History

Version	Author	Department	Date	Revision Comments
0.1	Fortian	N/A	June 2022	Document creation
0.2	Michael Tuton	Security	August 2022	Updates made per review of document
0.3	Michael Tuton	Security	October 2022	CEO review
0.4	Fortian	N/A	October 2022	Updates based on feedback (minor)
0.5	Michael Tuton	Security	June 2023	Annual review
0.6	James	Security	November 2023	Reviewed