

Best practices for keeping your data secure & compliant

1

Secure data collection

Limit the collection of personal or sensitive information to what is essential for your business operations. Opt for encrypted channels to ensure security of data collection.

2

Classify and prioritize data

Identify which data is sensitive, confidential, or public. Classify and prioritize data to ensure the most critical information is protected first.

Enforce access control

Limit access to sensitive data based on employee roles. Use MFA and role-based access controls to ensure only authorized personnel can access sensitive information.

Secure data backup

Periodically back up your critical data and consider using built-in backup features offered by many cloud services.

Train employees on data protection

Periodically conduct cybersecurity awareness training for all employees. Make sure they understand best practices for handling, storing, and sharing data securely.



**Change human cyber
security behavior with**

**security[®]
quotient.**

Singapore | India | Malaysia