

	BBW GLOBAL TEK PRIVATE LIMITED			ANNEXURE	
	APPROVED BY	DOCUMENT NO	ISSUE NO	ISSUE DATE	REVISION NO.
	MD	BBW/ANX/66	00	01/7/2025	01

INFORMATION SECURITY POLICY

1. Establishment of Internal Regulations and Policies Related to Information Security:

1.1. All employees, contractors, and third-party vendors must adhere to the established information security regulations and policies.

1.2. Information security regulations and policies will be regularly reviewed and updated to address evolving threats and technological advancements.

1.3. Designated personnel will be responsible for enforcing compliance with information security regulations and policies.

2. Awareness Training to Prevent Information Security Breaches:

2.1. Mandatory information security awareness training will be provided to all employees upon hiring and periodically thereafter.

2.2. Training sessions will cover topics such as password security, phishing awareness, data handling procedures, and physical security measures.

2.3. Employees will be required to complete refresher training sessions annually to ensure ongoing awareness and compliance.

3. Whistleblowing Procedures to Prevent Information Security Breaches:

3.1. An anonymous reporting mechanism will be established for employees to report suspected information security breaches or violations.

3.2. Reports will be thoroughly investigated, and appropriate actions will be taken to address any identified breaches or violations.

3.3. Non-retaliation policies will be enforced to protect whistleblowers from adverse consequences.

4. Incident Response Plan (IRP) to Manage Confidential Information Breaches:

4.1. An incident response team will be designated and trained to promptly respond to and mitigate information security incidents.

	BBW GLOBAL TEK PRIVATE LIMITED			ANNEXURE	
	APPROVED BY	DOCUMENT NO	ISSUE NO	ISSUE DATE	REVISION NO.
	MD	BBW/ANX/66	00	01/7/2025	01

4.2. The IRP will include procedures for assessing the scope and impact of breaches, containing incidents, and restoring affected systems and data.

4.3. Communication protocols will be established to notify relevant stakeholders, including customers and regulatory authorities, in the event of a breach.

5. Perform Information Security Risk Assessments:

5.1. Regular risk assessments will be conducted to identify potential vulnerabilities and threats to information security.

5.2. Risk assessments will consider factors such as data sensitivity, system access controls, and external threats.

5.3. Mitigation strategies will be developed and implemented to address identified risks.

6. Implement a Record Retention Schedule:

6.1. A record retention schedule will be established to govern the retention and disposal of confidential information in compliance with legal and regulatory requirements.

6.2. Document retention periods will be determined based on the nature of the information and applicable legal mandates.

6.3. Procedures will be implemented to securely store and dispose of records according to the retention schedule.

7. Measures to Protect Customers/Third Parties from Unauthorized Access or Disclosure:

7.1. Access controls will be implemented to restrict unauthorized access to customer and third-party information.

7.2. Encryption and other security measures will be employed to safeguard sensitive data during transmission and storage.

7.3. Regular security audits will be conducted to ensure compliance with established protective measures.

8. Procedure for Obtaining Stakeholder Consent for Processing, Sharing, and Storage of Confidential Information:

8.1. Clear and transparent procedures will be established for obtaining stakeholder consent for the processing, sharing, and storage of confidential information.

	BBW GLOBAL TEK PRIVATE LIMITED			ANNEXURE	
	APPROVED BY	DOCUMENT NO	ISSUE NO	ISSUE DATE	REVISION NO.
	MD	BBW/ANX/66	00	01/7/2025	01

8.2. Stakeholders will be provided with detailed information regarding the purpose and scope of data processing activities, as well as their rights and options for consent.

8.3. Consent obtained will be documented and maintained in accordance with record retention policies.

This Information Security Policy is designed to promote a culture of security awareness, compliance, and accountability throughout the organization. All employees are expected to familiarize themselves with this policy and uphold its principles in their daily activities. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.



01/7/2025

Managing Director