Data Protection Policy

HIVE

INTRODUCTION AND PURPOSE

1. At HIVE Property, we are committed to protecting the privacy and security of personal and sensitive data entrusted to us. This Data Protection Policy outlines our principles and practices for the collection, processing, storage, and protection of data to ensure compliance with applicable data protection laws and regulations. The purpose of this policy is to establish a framework that safeguards data privacy rights and maintains the confidentiality, integrity, and availability of the data we handle.

SCOPE

2. This policy applies to all employees, contractors, and third-party service providers who handle personal and sensitive data on behalf of HIVE Property. It covers all data processing activities conducted within our organization, regardless of the format or medium in which the data is stored or transmitted.

COMPLIANCE WITH LAWS AND REGULATIONS

3. We are committed to complying with all applicable data protection laws, regulations, and industry standards, including but not limited to the Privacy ACT 1988 and the Data Protection ACT 1998 and any other relevant regional or sector-specific data protection requirements.

DATA COLLECTION AND PROCESSING

4.1. Purpose Limitation and Consent: We collect and process personal data only for specific, legitimate, and lawful purposes. We ensure that individuals are informed about the purpose of data collection and obtain their explicit consent where required by law.

4.2. Data Minimization: We collect and process only the minimum amount of personal data necessary to fulfill the specified purpose. We avoid collecting unnecessary or excessive data.

4.3. Lawful Basis for Processing: We ensure that we have a valid legal basis for processing personal data, such as the necessity for contract performance, compliance with legal obligations, or consent obtained from the data subject.

DATA STORAGE AND RETENTION

5.1. Data Security Measures: We implement appropriate technical and organizational measures to protect personal data against unauthorized access, disclosure, alteration, or destruction. These measures include encryption, access controls, network security, regular security audits, and staff training on data protection best practices.

5.2. Data Retention: We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required by law. We regularly review and update our data retention practices to ensure compliance with legal requirements.

5.3. Data Disposal: When personal data is no longer needed, we securely dispose of it using approved methods, including physical destruction and secure deletion of electronic records.

DATA ACCESS AND SHARING

6.1. Data Access Controls: Access to personal data is granted only to authorized personnel who require it for legitimate business purposes. Access permissions are regularly reviewed and updated based on the principle of least privilege.

6.2. Third-Party Data Sharing: We may share personal data with third-party service providers or partners who have entered into appropriate agreements ensuring the protection and confidentiality of the data. We conduct due diligence on these third parties to ensure their compliance with applicable data protection standards.

INDIVIDUAL RIGHTS

7.1. Data Subject Rights: We respect the rights of individuals regarding their personal data. We facilitate the exercise of rights such as the right to access, rectify, erase, restrict processing, object to processing, and data portability in accordance with applicable data protection laws.

7.2. Data Subject Requests: We have established procedures to handle data subject requests and respond to them promptly and in compliance with legal requirements. We maintain transparent and effective communication with individuals regarding the processing of their personal data.

DATA BREACH RESPONSE

8.1. Data Breach Management: In the event of a data breach, we have established procedures to identify, assess and mitigate the impact of the breach. We promptly investigate and take appropriate actions to minimize harm and prevent future incidents.

8.2. Incident Response Team: We maintain an incident response team comprising relevant stakeholders from IT, legal, security, and other pertinent departments. This team is responsible for coordinating the response to data breaches and ensuring a timely and effective resolution.

8.3. Reporting and Communication: We have a reporting mechanism in place for employees and third parties to report any actual or suspected data breaches. All incidents should be reported to the incident response team as soon as possible. We maintain clear lines of communication with affected individuals, regulatory authorities, and other relevant stakeholders as required by applicable laws and regulations.

8.4. Breach Assessment: Upon discovering a data breach, we conduct a thorough assessment to determine the nature and scope of the incident, including the type of data affected, the potential risk to individuals, and the underlying cause of the breach. This assessment helps us evaluate the severity of the breach and prioritize response actions.

8.5. Mitigation and Remediation: We take immediate steps to contain the breach, mitigate any ongoing harm, and restore the security and integrity of the affected systems and data. This may involve isolating affected systems, changing access credentials, applying patches or updates, or other necessary remedial actions.

8.6. Notification and Reporting: If required by applicable laws and regulations, we notify affected individuals, regulatory authorities, and other relevant stakeholders about the breach in a timely manner. Our notifications provide clear and concise information about the breach, its impact, and the steps individuals can take to protect themselves.

8.7. Learnings and Improvements: Following a data breach, we conduct a post-incident review to identify lessons learned and areas for improvement. This review helps us enhance our security measures, update policies and procedures, and provide additional training to employees to prevent similar incidents in the future.

8.8. Record Keeping: We maintain records of all data breaches, including the nature of the breach, the actions taken, and any remedial measures implemented. These records help us demonstrate our compliance with data protection laws and facilitate future audits or investigations.

TRAINING AND AWARENESS

9.1. Employee Training: We provide regular training and awareness programs to all employees regarding their responsibilities in safeguarding personal data, recognizing potential data breaches, and following established procedures. Training is tailored to employees' roles and includes updates on emerging threats and best practices in data protection.

9.2. Policy Awareness: We ensure that all employees are aware of this Data Protection Policy and understand their obligations to comply with its provisions. We provide accessible and clear information about the policy, including its purpose, key principles, and reporting mechanisms.

POLICY REVIEW AND UPDATES

10.1. Policy Review: We regularly review this Data Protection Policy to ensure its continued relevance and compliance with applicable data protection laws and regulations. Reviews take into account changes in the organization's activities, emerging risks, and evolving best practices in data protection.

10.2. Policy Updates: Any necessary updates or amendments to this policy are communicated to all relevant stakeholders and incorporated into our practices promptly. Employees are informed of policy changes and provided with necessary guidance or training to ensure their adherence.

By implementing and adhering to this Data Protection Policy, we aim to create a secure and privacy-conscious environment that safeguards personal and sensitive data while complying with legal and regulatory requirements.