Data protection and data security policy (v1.0)

Introduction: The Data Protection and Data Security Policy outlines our commitment to protecting the confidentiality, integrity, and availability of our data. This procedure is designed to ensure that we comply with all relevant data protection and security laws and regulations, and to minimize the risk of unauthorized access, use, or disclosure of our data.

Scope: This procedure applies to all employees, contractors, and third-party service providers who handle or have access to our data, whether in electronic or paper form.

Roles and Responsibilities: It is the responsibility of all employees to comply with this procedure and to protect the confidentiality, integrity, and availability of our data. The Data Protection Officer (DPO) is responsible for overseeing compliance with this policy and ensuring that appropriate controls are in place to protect our data. All employees are required to report any suspected or actual data breaches or security incidents to the DPO as soon as possible.

Data Classification: All data must be classified based on its sensitivity, value, and potential impact on the organization. This includes personal data, financial data, and confidential business information. Data should be classified as public, internal, confidential, or restricted, and appropriate access controls and security measures should be implemented based on the classification.

Data Access: Controls Access to data should be granted on a need-to-know basis, and all employees should have a unique username and password to access our systems. Access should be reviewed regularly, and access privileges should be revoked promptly when they are no longer required.

Data Storage and Transmission: All data should be stored in secure locations and protected with appropriate physical and technical controls. Data should be encrypted when it is transmitted over public networks or stored on portable devices, such as laptops or USB drives.

Data Retention and Disposal: Data should be retained only for as long as necessary to fulfill its intended purpose and in compliance with legal and regulatory requirements. When data is no longer required, it should be disposed of securely to prevent unauthorized access or disclosure.

Data Breach Management: In the event of a suspected or actual data breach or security incident, all employees should report the incident to the DPO as soon as possible. The DPO will investigate the incident and take appropriate action, which may include notifying affected individuals, law enforcement, or regulatory authorities.

Training and Awareness: All employees should receive regular training on data protection and data security policies and procedures, including their roles and responsibilities for protecting our data.

Monitoring and Review: This policy and procedure will be reviewed regularly to ensure that it remains effective and relevant. The DPO will monitor compliance with this procedure and report on any non-compliance or incidents to senior management.

Conclusion: This procedure is designed to protect the confidentiality, integrity, and availability of our data and to ensure compliance with all relevant data protection and security laws and regulations. All employees are responsible for complying with this procedure and for protecting our data.

Signed,

Bill Pu, President of Leopard Imaging Inc.