# PV Generation Ltd IT Policy

1. Purpose:

The purpose of this IT policy is to outline the guidelines and best practices for the use of information technology resources at PV Generation Ltd. This policy is designed to ensure the security and integrity of our data, compliance with Ireland's data protection laws, and the efficient use of IT resources.

2. Scope:

This policy applies to all employees, contractors, and third-party vendors who have access to PV Generation's IT resources, including but not limited to computers, networks, software, and data. It also applies to all devices used for work-related activities.

3. Acceptable Use of IT Resources

3.1. Authorized Access: Users must only access IT resources that they are authorized to use. Access to sensitive data should be restricted on a need-to-know basis.

3.2. Password Security: Users are not allowed to change the passwords for further information contact to IT department, and not share them with others. Multi-factor authentication (MFA) should be enabled wherever possible.

3.3. Software Usage: Only authorized software and applications should be installed on company devices. Personal software downloads are not permitted.

3.4. Data Backups: Regular backups of critical data should be performed to prevent data loss. Data backup procedures must be followed diligently.

3.5. Email Usage: Company email accounts must be used for business purposes only. Employees should exercise caution when clicking on email attachments or links, especially if they appear suspicious.

4. Data Protection and Privacy

4.1. GDPR Compliance: PV Generation complies with the General Data Protection Regulation (GDPR) and other relevant data protection laws. Employees are required to handle customer data with care and report any data breaches promptly.

4.2. Data Classification: Data should be classified based on its sensitivity, and appropriate security measures should be applied accordingly. Confidential or personal data should be encrypted and stored securely.

4.3. Data Retention: Data should be retained only as long as necessary and in compliance with applicable laws and regulations. Unused or outdated data should be securely disposed of.

5. Security Measures

5.1. Anti-Virus and Anti-Malware: All devices connected to the company network must have up-to-date antivirus and anti-malware software installed.

5.2. Firewalls: Firewalls should be enabled and configured to protect the network from unauthorized access.

5.3. Updates and Patching: Operating systems and software should be regularly updated with security patches to address vulnerabilities.

6. Mobile Device and Remote Work Security

6.1. Mobile Device Management (MDM): Mobile devices used for work purposes should be enrolled in the company's Mobile Device Management system for security and remote management.

6.2. Remote Access: When working remotely, employees should use secure VPN connections to access company resources.

7. Reporting Security Incidents

Employees must promptly report any security incidents, breaches, or suspicious activities to the IT department or their supervisor.

8. Enforcement

Failure to comply with this IT policy may result in disciplinary action, up to and including termination of employment.

9. Review and Updates

This IT policy will be periodically reviewed and updated to reflect changes in technology, laws, and business requirements.

For questions or concerns related to IT security or this policy, contact the IT department at info@pvgeneration.ie