# PSMG LIMITED INFORMATION SECURITY POLICY STATEMENT

At PSMG, we may hold personal data about employees, clients, suppliers, and other individuals for a variety of business purposes. Our information security system is designed to protect the company, its employees, partners, and customers from illegal or damaging actions, whether deliberate or accidental, when processing data and using business equipment. We are committed to ensuring that any data we handle is secure, and we are fully compliant with the General Data Protection Regulation (GDPR) and registered with the Information Commissioner's Office (ICO).

## SCOPE

This policy applies to all PSMG employees, contractors, and individuals who have access to the company's electronic systems, information, software, and hardware, whether on a permanent or temporary basis. The policy covers the processing of information in any form or media used in the company's operations, both internal and external, and applies to all data/information processed within the company, including third-party relationships.

## CONFIDENTIAL INFORMATION

Confidential information includes, but is not limited to:

1. Financial data
2. Internal business information
3. Client, partner, and supplier data
4. Patents, technologies, and intellectual property
5. Existing and prospective customer/client information

## PERSONAL AND COMPANY DEVICES

Employees must ensure the security of both personal and company devices:

1. Keep all devices password-protected and ensure passwords are strong and regularly updated.
2. Use antivirus software and ensure it is regularly updated.
3. Ensure that devices containing sensitive information are never left exposed or unattended.
4. Log into company accounts and systems only through secure networks (e.g., VPNs).

5. Be cautious when opening email attachments or clicking on links from unknown or untrusted sources.

6. Do not install, copy, distribute, or store illegal software or unlicensed content on PSMG devices or systems.

7. Limit the storage of confidential information on personal or company devices to what is necessary for specific tasks.

8. Never store company or third-party information on personal devices without prior consent from Top Management.

9. Share client/customer/supplier data only with authorised personnel.

10. Only collect and process the minimum amount of personal data necessary for business purposes.

11. Be wary of clickbait and phishing attempts.

12. Ensure that recipients of shared data are authorised to access it.

13. Avoid transferring sensitive data unless absolutely necessary and ensure it is encrypted.

14. Do not share confidential information over unsecured networks or with unauthorised individuals.

15. Immediately report any suspicious activities, scams, security breaches, or loss of equipment containing sensitive information.

16. Always lock screens or close confidential documents before leaving your workstation.

17. Do not download software without approval from Top Management.

18. Use the internet in compliance with applicable laws, and understand that usage may be monitored by Top Management.

19. Use personal social media responsibly and refrain from disclosing any workplace-related information that could compromise company security.

## DATA STORAGE

All data, whether in paper, electronic, or other forms, must comply with the requirements outlined in this policy. The company will adhere to all relevant statutory regulations for the collection, processing, protection, and retention of data.

## DATA RETENTION

We will retain personal data only for as long as necessary, taking into account the specific purpose for which the data was collected. The retention period will be determined in accordance with our data retention guidelines and the requirements of applicable laws.

## REPORTING SECURITY INCIDENTS

Any security incidents or suspected breaches involving information/data processing must be reported to management immediately. Management will take the necessary steps to prevent further damage, address the issue, and restore the security of the company's data.

Jason Silcox

Business Director
January 2025