APOGEE
An HP Company

Apogee Information Security Policy Statement

This policy statement outlines Apogee's unwavering commitment to Information Security Management (ISM) and the ongoing development and maturity of our Information Security Management System (ISMS).

Under the leadership of the Chief Executive Officer (CEO) and with the direct oversight of the Executive Leadership Team, we are fully committed to establishing, implementing, maintaining, and continually improving our ISMS. This ensures that information security is managed effectively across all aspects of Apogee's diverse operations, including the secure handling of personal data, the management of privileged access, and the robust protection of all client and internal information across our Managed Print Services, Managed IT Services, Outsourced Document Services, and Digital Transformation offerings.

To drive operational excellence and continuous improvement, the IT Director, as the head of the Data Security Group, is specifically delegated the authority and responsibility for monitoring the effectiveness and driving the continual improvement of our ISMS. This includes regularly reviewing our security posture, identifying areas for enhancement, and implementing necessary changes to adapt to evolving threats and maintain our robust security standards.

Our purpose is to clearly communicate our ISM expectations to all stakeholders, including our employees, temporary staff, contractors, business partners, and visitors. We expect everyone to deliver services on our behalf or working on our premises to share our commitment. While some aspects of our operations, such as handling personal data and having privileged access, present clear and specific information security requirements, we expect all client and internal hard copy and electronic information to be treated in a secure manner throughout all our processes.

Our overall ISM objective is to protect the organisation from incidents that might have an adverse effect on the people we work with, our business operations, and our professional standing. Information Security issues can include:

- **Confidentiality**: preventing inappropriate access to or disclosure of information.
- **Integrity**: safeguarding against information being altered or erroneously validated, whether deliberate or accidental.
- **Availability**: ensuring information is accessible when and where it is required by authorised individuals.
- **Privacy**: protecting Personally Identifiable Information (PII) from unauthorised access or disclosure.

Many types of incidents can pose a threat to our effective use of information, impacting aspects like performance, consistency, reliability, accuracy, and timeliness. More detailed ISM objectives and monitoring will be defined separately to this policy, either within a stand-alone document or within management review processes.

Our information security management system will systematically assess and manage ISM risks. We shall also understand and comply with any applicable ISM or related legal/regulatory requirements across all jurisdictions in which we operate.

This statement has been prepared to demonstrate Apogee's commitment to continual improvement in information security. The Executive Leadership Team shall regularly review the effectiveness of the ISMS and establish or review objectives, targets, and appropriate actions to achieve the intended outputs of the ISMS. This message shall be communicated and understood throughout Apogee, and it is expected that all persons performing work on our behalf share a commitment to these values.

This Policy Statement shall be made available to the public, upon request, and shall be communicated and adhered to by all employees, temporary staff, contractors, and visitors who interact with our information assets or enter any of our worksites.

This policy has been approved & authorised by:

Name:	James Clark
Position:	Chief Executive Officer
Date:	28/05/2025
Signature:	James Clark James Clark (May 28, 2025 13:15 GMT+1)