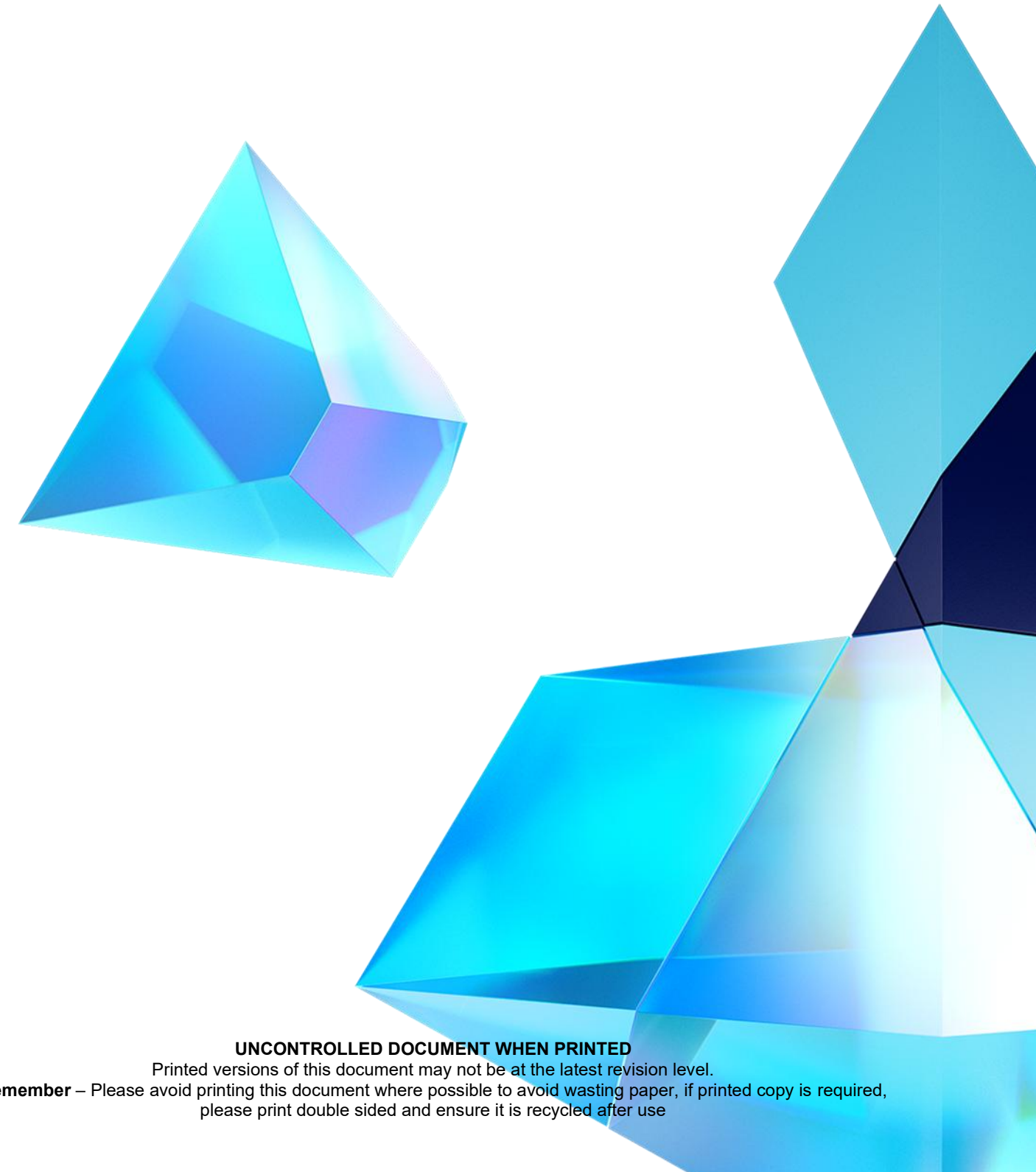
Impellam Group

Believe in the **power of work**

IMPELLAM GROUP

SUPPLIER INFORMATION SECURITY STANDARDS

Date: June 2026



UNCONTROLLED DOCUMENT WHEN PRINTED
Printed versions of this document may not be at the latest revision level.
Remember – Please avoid printing this document where possible to avoid wasting paper, if printed copy is required, please print double sided and ensure it is recycled after use

OUR MISSION IS TO BE THE WORLD'S MOST TRUSTED WORKFORCE AND STEM TALENT SOLUTIONS GROUP.

We believe in the power of work.

Through the power of work, we build better businesses and help people lead more fulfilling lives.

At Impellam we are united by one purpose, one culture, one driving force. We call it Virtuosity. It's how we do what we do. It's why we're different. It's our determination to do even more and to always be ambitious and brave for all our stakeholders.

Impellam Group Limited and its associated companies (www.impellam.com) requires all suppliers, consultancies, companies **("Supplier(s)")** providing information processing products and/or services to adhere to these Information Security Standards to ensure our mission is embedded throughout the supply chain.

Suppliers represent a critical component of Impellam's performance and value proposition. Suppliers that cannot or will not adhere to these Information Security Standards must immediately advise Impellam and may be disqualified as an Impellam supplier. Suppliers are expected to extend the same standards to their sub-contractors who will form part of the product and/or services being provided to Impellam.

POLICY STATEMENT

Key principles of these Information Security Standards include the following:

- Ensuring confidential and personal data is treated appropriately;
- Vulnerabilities in software is managed adequately;
- Risks are monitored and assessed;
- Clear plans are made for incident response;
- Security of information is controlled and maintained.

CONFIDENTIALITY

Suppliers agree to maintain the confidentiality, integrity and availability of all information and/or information processing systems entrusted to the Supplier by Impellam, including but not limited to personally identifiable information (PII), sensitive data, trade secrets, and proprietary information.

DATA PROTECTION

Supplier agrees to implement appropriate technical and organisational measures to protect the confidentiality, integrity and availability of Impellam's data, in accordance with relevant data protection laws and utilising controls outlined in ISO/IEC 27001:2022 and/or SOC2, or an equivalent, as a baseline. For cloud-based services, Supplier shall ensure compliance with industry best practices and standards for cloud security. For example, Cloud Security Alliance (CSA) Security Guidance and the EU Cloud Code of Conduct.

ACCESS CONTROL

Supplier shall implement, maintain and regularly review physical and logical access controls including supplier user access rights to ensure that only authorized personnel have access to Impellam's information, and such access is granted based on the principle of least privilege. Access controls and Supplier user access rights must be reviewed whenever there is any reason to suspect they may have been compromised.

INCIDENT RESPONSE

Supplier shall operate incident detection and management controls in line with the requirements of ISO/IEC 27001:2022 and/or SOC2 and shall promptly notify Impellam within 24hrs of a confirmed security incident or breach affecting Impellam's data and shall cooperate with Impellam in investigating and resolving such incidents.

RISK MANAGEMENT

Supplier shall conduct regular risk assessments and take necessary measures to mitigate identified risks to Impellam's information assets, utilising controls outlined in ISO/IEC 27001:2022 and/or SOC2, or an equivalent, as a baseline. Supplier shall perform regular and impartial security assessments and audits of their infrastructure and services against their selected security baselines, including cloud infrastructure where cloud services are provided and take the necessary mitigating steps required for any non-conformities that arise.

VULNERABILITY MANAGEMENT

Supplier shall promptly inform Impellam of any relevant vulnerabilities in its systems and/or products that may affect the confidentiality, integrity and/or availability of information entrusted to it by Impellam. If the vulnerability cannot be immediately rectified, Supplier shall provide relevant guidelines on recommendations to Impellam for compensating controls until the vulnerability can be rectified. Supplier commits to maintaining an effective vulnerability management program for its own systems and any relevant software or services that it develops, including timely patching and updates, vulnerability scanning, and penetration testing. Remediation timeframes for identified vulnerabilities shall align with the Cyber Essentials scheme guidelines, ensuring that critical and high vulnerabilities are remediated within 14 days and lower-risk vulnerabilities within 30 days.

COMPLIANCE REPORTING

Supplier shall provide Impellam with contact information of person(s) who can provide evidence of adherence to security controls and update Impellam whenever that contact information changes. The contact must respond within five working days to any request from Impellam for information relating to information security controls and provide the requested information within 10 working days.

Supplier must provide Impellam with an appropriately redacted summary list of its security controls and where applicable, a copy of its ISO 27001:2022 compliant Statement of Applicability identifying which Annexe A controls are specifically excluded and justifications for their exclusion, and the methods through which the requirements of included/selected controls are met (e.g. names of relevant policies, or processes etc.)

ACCREDITATIONS/CERTIFICATIONS

Supplier shall follow the principles of, and where applicable hold and maintain, Information Security standards and certifications such as, but not limited to ISO/IEC 27001:2022, SOC2 Type 2 or equivalents.

IMPELLAM'S COMMITMENT TO SUPPLIERS

Impellam promises to adhere to the same standards in its dealings with Suppliers and their information. For those Suppliers who meet the high standards required to become an Impellam Supplier, we request your co-operation to mutually hold each other accountable. Impellam wants to be recognised as your customer of choice and welcomes open and honest feedback.

If you have any questions regarding this document, please contact ITGovernance@Impellam.com

Document History

Date	Version	Edited/reviewed by	Approved by	Changes
01/06/24	1.0	Faye Lemiere	Emma Trew	First published version
01/06/25	1.1	Andy Cousins		Annual review & reapproval. No changes.
24/06/26	1.2	Andy Cousins	Emma Trew	Added reference to SOC2 as an alternative to ISO 27001. Clarified applicability of vulnerability management to include developed products & services.