IT-CP-GBL03 IT Security Policy for Acceptable Usage Summary

This Document is a summary of IT-CP-GBL01 IT Security Policy for Acceptable Usage and IT-CP-GBL02 Artificial Intelligence Acceptable Usage Policy, this will be an external facing document.

Approval*

Role	Name	Function
Document Owner	Cole Sinkford	CISO

* Approval with time stamp is maintained in the GF IT Document Framework

Subject Matter Expert	James Colelli Ponnusamy Ponrajesh Raunaq Gangahar Ajith Kunju Raman	IT Compliance
	Balaji Ramammoorthy	Third Party Risk Management

Purpose of the Document:	GlobalFoundries ("GF") is committed to protecting the confidentiality, integrity, and availability of information entrusted to us by our customers, suppliers, partners, and workforce, and to ensuring the responsible, ethical, and secure development and use of artificial intelligence (AI). This policy sets forth GF's high-level commitments to information security and responsible AI governance in alignment with applicable laws, regulations, and recognized international standards.
Scope:	This policy applies globally to GF and covers information assets, digital systems, and AI systems developed, deployed, or used by GF, including those operated by third parties on GF's behalf. It is intended as an external, public facing statement of GF's commitments and is supported by internal standards, procedures, and governance mechanisms.
Responsibilities:	The Management of GF IT is responsible for compliance to this document. This document should be reviewed after changes in the respective global standard and after local changes, but at least at the frequency stated in the GF IT Documentation Procedure by the responsible document owner and document controller.

Contents

IT-CP-GBL03 IT Security Policy for Acceptable Usage Summary

IT-CP-GBL01 IT Security Policy for Acceptable Usage-Appendix01

1 Information Security Policy

Information Security Commitment
GF maintains a comprehensive information security management framework designed to continuously strengthen protection against evolving threats and risks.

We commit to:

- **Continuous improvement of information security systems** through risk assessments, governance reviews, and management system enhancements, including the use of internationally recognized standards (e.g., ISO 27001) and the Plan-Do-Check-Act cycle. For more information on the attained Certifications – click here.

- **Ensuring the integrity, confidentiality, and protection of data** across its lifecycle, from creation and use through retention and secure disposal, using information classification, access controls, and technical safeguards.

- **Monitoring, detecting, and responding to information security threats** through layered cybersecurity defenses, incident response planning, and business continuity measures designed to minimize operational and data impacts.

- **Deepening information security awareness** through companywide security awareness programs, including mandatory training, ongoing communications, and simulated social engineering and phishing exercises, to reinforce individual responsibility and promote secure behaviors in daily operations.

1.1 Roles and Responsibilities

Information security is a shared responsibility across GF:

- All employees, contractors, and authorized users are responsible for protecting GF information and complying with applicable policies and security requirements.

- Executive leadership and the Chief Information Security Officer (CISO) oversee the information security program, governance, and enterprise risk management.

- Dedicated information security and compliance teams implement controls, conduct monitoring, and support incident response and continuous improvement activities.

1.2 Third-party Information Security

GF requires suppliers, service providers, and other third parties with access to GF information or systems to comply with defined information security requirements. These expectations are communicated through contractual obligations, supplier standards, and ongoing risk management activities to help safeguard GF and customer data throughout the supply chain.

IT-CP-GBL01 IT Security Policy for Acceptable Usage-Appendix01

2 Responsible AI Policy

Responsible AI Principles
GF recognizes the potential of AI to support innovation and operational excellence and is committed to its responsible use.

Our approach to AI is guided by the following principles:

- **Respect for data privacy:** AI systems are designed and used in alignment with data protection laws and privacy by design principles, limiting data collection and use to legitimate, authorized purposes.

- **Cybersecurity and system integrity:** AI systems and supporting infrastructure are protected through secure by design practices, reliability testing, and lifecycle security controls.

- **Avoidance of bias and unfair outcomes:** GF seeks to identify and mitigate potential bias in AI data, models, and outputs by applying fairness objectives, testing, and review prior to deployment and during use.

- **Human oversight and intervention:** Qualified humans remain accountable for critical decisions supported by AI, with mechanisms in place to enable review, challenge, and intervention where appropriate.

- **Transparency and explainability:** GF promotes transparency by disclosing the use of AI where required and providing meaningful explanations of AI supported outcomes, limitations, and intended use.

- **Clear accountability:** Each AI system has defined ownership and governance, with accountability for outcomes aligned to GF's internal review, approval, and compliance processes.

- **Defined use boundaries:** GF defines and enforces boundaries for acceptable AI use and will not deploy AI systems that engage in manipulative behavior, exploitation of vulnerabilities, social scoring, or unauthorized biometric surveillance, consistent with emerging regulatory frameworks.

2.1 Governance and Oversight

GF maintains governance structures to oversee AI-related risks, ethics, and regulatory compliance. The Artificial Intelligence Ethics & Regulatory Committee provides guidance, reviews AI use cases, and helps ensure alignment with applicable regulations, GF's Code of Conduct, and recognized ethical standards.

IT-CP-GBL01 IT Security Policy for Acceptable Usage-Appendix01

3 Policy Review:

This Policy will apply for an unlimited period and is governed under GlobalFoundries' corporate policy framework. The Policy Owner is responsible for ensuring that the policy is periodically reviewed and maintained. Updates to the policy are subject to appropriate review and approval by executive management, and new policies or significant changes are endorsed by the relevant Board committee, as applicable. GF remains committed to continuous improvement in information security and responsible AI practices through monitoring, oversight, and governance enhancements.

4 Compliance

Information Security may perform a review or assessment of the policy to verify compliance and appropriate procedural controls are in place. If the review or assessment finds non-compliance, functional business owners will be notified and required to take the necessary actions to correct the non-compliance within a reasonable timeframe. The timeframe will be determined jointly by Information Security and the functional business owner.

The decision of whether existing controls are adequate is determined by the Information Security team.

Change History					
Version	Name	Date	Type	Paragraph	Remarks
01	James Colelli Balaji Ramamoorthy Ajith Kunju Raman	2026-04-29	N	All	New Document

Legend: N = New C = Change R = Removed