

Gamma Group Information Security Policy

Gamma Communications plc (“Gamma”)

Introduction

Gamma recognises the severe risk posed by cyber threats to our customers, operations, assets, and employees. Gamma may be targeted directly to fulfil a criminal's objectives but more likely indirectly to impact one or more of our customers.

According to the World Economic Forum's World Economic Forum's Global Risks Report 2024¹ Cyber insecurity' will remain a top ten global risk for the next ten years. This is due to the ever-evolving dependency society has on technology and the equally evolving threat landscape that enables criminals to commit crimes.

Information or cyber security is a set of controls used to address the risks and threats that may impact Gamma. Threats can originate from multiple avenues: external attacks, physical intrusion, insider compromise and the impact is exacerbated by poor or inconsistent controls.

Aims and Goals

The aim of this policy is to inform the Gamma Group how security risks will be managed.

Gamma's goal is to alleviate the security risk faced by following these four steps:

- a. Identify security threats, vulnerabilities, and risks.
- b. Protect against security threats and risks.
- c. Detect security threats.
- d. Respond to security threats and incidents, including full business recovery when required.

Scope

Gamma Group employees, Gamma suppliers and customers.

Policy statements

1. Gamma ensures security is part of the company's objectives, and day to day activities.
2. Gamma has a low-risk appetite for cyber security risk and ensures resources and investment are made available to protect Gamma systems and assets appropriately.
3. Gamma will comply with local legislation, regulation, and contractual obligations regarding security controls.
4. Products, services and supporting systems will be managed to assure the security and resilience of systems and assets.
5. Gamma will ensure Group data is protected using appropriate security controls
6. Whenever possible security controls will be systemised to ensure they are easily enforced.

¹ Global Risks Report 2024 | World Economic Forum | World Economic Forum

7. Gamma will risk assess third parties who pose a security risk to Gamma assets.
8. Whilst Gamma aims to prevent cyber-attacks, we acknowledge they can occur, and will invest in response capabilities that allow us to recover as quickly as possible.
9. Gamma will actively participate in industry relationships to support information sharing, risk reduction and improve restoration activities.

Governance and reporting

The Board, and its sub committees, receive briefings on severe security threats impacting Gamma.

The Group Security Director completes a monthly review of security controls to ensure Gamma is maturing at the right pace considering external and internal threats. This review is informed by the Head of Security Operations and the Head of Security Engineering.

Gamma Group aligns to, or is certified against, various security frameworks including NIST Cyber Security Framework (CSF), ISO 27001 and Cyber Essentials Plus.

Responsibilities

Role	Responsibility
All managers and employees	Responsible for the appropriate control of data they manage on a day-to-day basis
Group Business Continuity team	Responsible for ensuring data is considered during business impact analysis activities.
Group Risk Management Team	Responsible for ensuring appropriating processes are in place to risk assess suppliers and third parties.
Group Security Director	Accountable for the security controls within the Gamma Group
Group Security Teams	Responsible for outlining appropriate operational data protection controls.
Technology and Operations teams	Responsible for the implementation of relevant security controls.

Adoption

Those who believe there has been a breach of the security controls should raise their concerns as a security incident via the IT Service Desk.

Employees who wilfully breach security controls may face disciplinary action.

Enforcement of security expectations for suppliers should, where possible, come from contractual clauses.

Document Control

Classification:	Public - Published
Document Ref:	G-RG-POL-004
Document Owner:	Colin Lees, Chief Technology Officer
Effective Date:	06 February 2025
Version:	1.3
Approved by:	The Gamma Board