Gamma Group Information Security Policy

Document Control

Classification:	**Public - Published**
Document Ref:	G-RG-POL-004
Document Owner:	Risk & Governance
Effective Date:	Aug-22
Version:	1.0
Approved by:	John Murphy - Group Operations Director
Reference Documents:	[G-RG-POL-002] - Group Risk policy

Contents

Gamma Group Information Security Policy 1

Document Control *1*

Contents *1*

Introduction *2*

Aims and Goals 2

Scope 2

Policy statements *2*

Governance and reporting *3*

Responsibilities *3*

Adoption *3*

Exemptions management *3*

Glossary *3*

Introduction

Gamma's mission is to provide straightforward cloud communication and collaboration services for business, underpinned by a robust, secure network.

Gamma recognises the high risk posed by cyber threats to our products and services provided to customers, operations, assets, and employees. According to the UK National Cyber Security Centre (NCSC) annual Cyber Breach Survey '39% of UK businesses identified a cyber-attack[1]' in 2021. These attacks have 5 broad aims:

a. Crime for profit,
b. Disruption to operations,
c. Espionage for intelligence,
d. Activism to force action,
e. Manipulation to control the narrative.

Gamma may be targeted directly to fulfil any of these aims and indirectly to impact one or more of our customers.

Information or cyber security is a set of controls used to address 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. Identification of security threats, vulnerabilities, and risks.
b. Protection against security threats and risks.
c. Detection of security threats.
d. Response 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 appropriate 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 risk.
4. Products, services and supporting systems will be managed to ensure the security and resilience of systems and assets.
5. Whenever possible security controls will be systemised to ensure they are easily enforced.
6. Gamma will risk assess third parties who have access to Gamma assets
7. Whilst Gamma aims to prevent cyber-attacks we acknowledge they can occur despite preventative measures and will invest in response capabilities that allow us to recover as quickly as possible.

[1] Cyber Security Breaches Survey 2022 - GOV.UK (www.gov.uk)

8. Gamma will actively participate in industry relationships to support information sharing, risk reduction and improve restoration activities.

Governance and reporting

The Risk Committee (subcommittee of the Board) receive a quarterly security briefing, considering cybersecurity risks and controls and the Board receive an annual security briefing.

The Group Risk and Governance Director completes a monthly review of security controls to ensure Gamma is maturing at the right pace considering external and internal threats.

Gamma Group aligns to, or is certified against, various security frameworks.

Responsibilities

The Group Technical Security team are responsible for outlining appropriate operational security controls.

The Group Architecture Review Board will ensure security controls are considered in all relevant review activity.

The Group Risk team will ensure appropriate processes are in place to risk assess security risks, suppliers and third parties.

The Technology and Operations teams, which manage Gamma's security resources, are responsible for the implementation of relevant security controls.

All employees must read this policy and accept their responsibilities as relates to their role.

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.

Exemptions management

Time bound policy exemptions may be issued by the Policy Owner.

Glossary

Term	Defintion
Cyber security	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (NIST)
Cyber attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.(NIST)
Security control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. (NIST)
Security risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for

Term	Defintion
	unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. (NIST)
Security threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. (NIST)