Gamma Supplier Terms

Gamma Group - Acceptable Usage Policy

Introduction

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

Gamma relies on its people to provide a vast amount of the security that protects our products and services. This is delivered through positive, security-conscious behaviours.

All employees are expected to take responsibility for the security of Gamma including reading this policy before being provided with a Gamma managed device. employees are expected to adhere to the policy throughout their employment with Gamma.

These policies must be reviewed at least annually to ensure continued alignment to business objectives.

Policy Scope

All Gamma Group employees, including Group Contractors, Group Temporary employees, Group Agency employees

Policy

User IDs and Passwords

1. Employees shall keep their passwords private and not write down or share this information with others. Should they believe these details have been exposed to others then they must change their secure credentials and report this as a security incident.
2. Employees must not permit others to perform any activity with their user IDs, and they must not perform any activity with user IDs belonging to other employees (unless part of their formal role).
3. Employees must not store personal user IDs and personal passwords in clear-text (eg in text or Word files) on end user devices.
4. Employees must never set-up or employ script files that contain a stored version of a personal identification number (PIN), a password, or a user-ID which can be used to gain access to a Gamma Group information system.
5. Gamma Group systems enforce password policies that users must adhere to. Where a user has to set the password, it is advisable to use three random words, guidance on password creation can be found here.
6. **To help employees securely manage their passwords, a password manager can be downloaded from an approved software repository on corporate laptops.**

Securing Information

1. Employees must respect data classification labels on information shared with them. Those creating information must add data classification labels to Gamma information.
2. Gamma Group employees must respect non-disclosure agreements signed as part of their role within Gamma Group.
3. Employees must diligently protect all Gamma Group information specifically identified as trade secrets from unauthorized disclosure. Trade secrets must be identified as such prior to being disclosed to any employees.
4. Employees must not discard confidential or secret information in publicly accessible refuse containers. They must instead securely retain the information until it can be shredded or destroyed in a cross shredder.
5. Employees who use corporate end user devices should store data on one of the IT supported storage locations (e.g. One Drive) where backups are required.

Use for Unauthorised Activities

1. No company-owned or company-provided system may be knowingly used for activities that are considered illegal under UK, European or international law. The user may not use the corporate network and/or systems to:
    a. engage in any activities that may lead to embarrassment, loss of reputation, or other harm to Gamma or our customers
    b. engage in activities that may be deemed an invasion of privacy
    c. engage in activities that cause disruption to the workplace environment or create a hostile workplace d. engage in gambling activities
    d. download or disseminate illegal, defamatory, discriminatory, vilifying, sexist, racist, abusive, pornographic, threatening, obscene or otherwise inappropriate messages or media
    e. make fraudulent offers for products or services
    f. perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, peer to peer networking or other IT information gathering techniques when not part of the employee's job function
    g. install or distribute "pirated" software
2. Knowingly taking any actions to bypass or circumvent security is expressly prohibited. Using company owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited.
3. Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

End-User Computing (EUC)

1. Depending on the employee's job function a Gamma provisioned, and managed device may be provided to employees when joining Gamma. Where provided the device it is assigned to the member of Gamma and will be centrally managed by IT.
2. Employees must not install, or allow others to install, software on their Gamma end user device without receiving advance authorisation to do so from the Head of IT.

3. Use of remote desktop software and/or services is allowable if it is provided by Gamma, this allows Gamma to secure the service and reduce the risk to Gamma systems.
4. Employees should take reasonable efforts not to access Gamma data, and information that are not directly related to their job function. Existence of access does not imply permission to use this access.
5. Employees must not leave their Gamma device unattended without logging out, invoking a Pin or password protected screen saver, or shutting the device down.
6. When stored in a vehicle or in another unattended public place, employees must keep all end user devices out of sight.

Remote Working

1. Remote workers must follow all system security policies and procedures as though they were in Gamma Group offices. Including, but not limited to, end user device usage and appropriate data storage.
2. Where shredders are not available, please retain sensitive information until it can be shredded or destroyed in a cross shredder.
3. The security of Gamma Group property at an alternative work site, including at home, is just as important as it is at the office. To maintain the security of Gamma Group assets and information, all employees and users are responsible for:
    a. Locking workstations when unattended, securing devices such as laptops, tablets, and mobile phones when not in use.
    b. Vigilance against shoulder surfing and other methods of unauthorized access to information (e.g., looking over someone's shoulder, photographing sensitive data).
    c. Never sharing passwords with anyone, including colleagues.
    d. Being cautious of, and reporting phishing emails and other social engineering attempts to Security
    e. Reasonable precautions must be taken to protect Gamma Group hardware, software, and information from theft, damage, and misuse.

Mobile Devices (Bring your own device)

1. BYO devices must be enrolled in the central Gamma mobile device management platform, access to Gamma systems and information will otherwise be denied.
    a. BYO devices must be protected through password, PIN or biometrics, be kept up to date and lock automatically if idle.
    b. Gamma Group reserves the right to remove all company data from any BYO device should the device become compromised, lost or stolen.
    c. BYO devices can be connected to Gamma guest wireless networks only.
2. It is the employee’s responsibility to inform Gamma’s IT Service Desk should the BYO device become compromised, lost or stolen

General Communications

1. The following actions shall constitute unacceptable use of corporate communications systems. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable:

a. Spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes.
b. Maliciously manipulating email header information or attempting to impersonate another person.
c. Sending any information that is illegal under UK, or European law
d. Accessing another employee's account without:
    i. the knowledge or permission of that employee
    ii. the approval of the Chief People Officer in the case of an investigation,
    iii. when such access constitutes a function of the employee's normal job responsibilities
e. Sending communications that may cause embarrassment, damage to reputation, or other harm to Gamma.
f. Disseminating defamatory, discriminatory, sexist, racist, or threatening messages or media
g. Sending communications that cause disruption to the workplace environment or create a hostile workplace
h. Knowingly misrepresenting Gamma's capabilities, business practices, warranties, pricing, or policies i. Conducting non-company-related business

2. Employees must recognise that communications sent from a Gamma account reflects Gamma Group, and, as such, all communications must be professional and courteous.
3. Gamma may use methods to block what it considers to be dangerous communications or strip potentially harmful attachments as it deems necessary.
4. Gamma provided end user devices have strong anti-malware controls however employees should use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment or link.
5. Employees must use care when receiving communications from 3rd parties requesting services to be carried out, identity validation should be undertaken.
6. Employees should be advised that Gamma owns and maintains all legal rights to its communications systems and network, and thus any communications passing through these systems is owned by Gamma. Keep in mind that communications may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the employee should be advised that communications sent to or from certain public or governmental entities may be considered public record.
7. Employees are strictly forbidden from deleting communications to hide a violation of this or another company policy. Further, communications must not be deleted when there is an active investigation or litigation where that communication may be relevant.
8. All relevant accounts will be set up at the time a new hire starts with Gamma, or when a promotion or change in work responsibilities for an existing employee creates the need.
9. When an employee leaves Gamma, or his or her access is officially terminated for another reason, Gamma will disable the employee's access to the accounts. Gamma is under no obligation to block the accounts from receiving communications and may continue to forward inbound communications sent to that account to another employee or set up an auto-response to notify the sender that the employee is no longer employed by Gamma.
10. Broadcast communications to all staff or all managers must be signed off by the Internal Communications team.

Use of E-mail

1. Gamma group email addresses will be constructed in a standardised manner than will enable identification of an employee by first name or initial, and last name. standard formats to maintain consistency across Gamma:
2. Gamma Group does not carry out speculative investigations, as such all requests to search an employee's mailbox from a line manager or another employee, must be approved by the Chief People Officer.
3. All requests from an employee to access a shared mailbox must be made via the IT Service Desk and approved by the employee's line manager and owner of the shared mailbox.
4. When using a company email account, email must be addressed and sent carefully. Employees should keep in mind that Gamma loses any control of email once it is sent external to the Gamma network. Careful use of email will help Gamma avoid the unintentional disclosure of sensitive or non-public information.
    a. Employees must take care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists to avoid inadvertent information disclosure to an unintended recipient.
    b. Use of the "Bcc" function should be used when emailing more than one external recipient.
5. Gamma makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with Gamma's employees or customer base) and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.
6. It is Gamma's intention to comply with Privacy and Electronic Communications Regulations of 2003 governing the sending of mass emails. For this reason, as well as to be consistent with good business practices, Gamma requires that email sent to more than twenty (20) recipients external to Gamma have the following characteristics:
    a. The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honoured immediately.
    b. The email must contain a subject line relevant to the content.
    c. The email must contain contact information, including the full physical address, of the sender.
    d. The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.
7. Emails sent to company employees, existing customers (who have not previously unsubscribed), or persons who have already inquired about Gamma's services are exempt from the above requirements.
8. An email signature, contact information appended to the bottom of each outgoing email, is required and will be automatically added by the email system The contact details align to your Gamma's Global Address List entry.
    a. Gamma automatically adds an email disclaimer to the end of every outgoing external email message, this must contain the legally required notices.
9. Gamma recognises that employees may have personal email accounts in addition to their company provided account. The following sections apply to non-company provided email accounts:

a. Except in exceptional circumstances employees are prohibited from sending business email from a non-company-provided email account.
b. Employees are permitted to access external or personal email accounts from the corporate network, if such access is approved by your line manager.

Social Media

1. Blogging and social networking by Gamma's employees, on behalf of or regarding Gamma, are subject to the terms of Gamma policy, whether performed from the corporate network or from personal systems.
2. Unless requested as part of a formal promotional activity employees must not post Gamma Group work related items - including pictures, names, product information or commentary on any company activity - on Social Networking or file sharing web sites.

Telephones and Voice Mail

1. Workers must not record messages containing sensitive information on answering machines or voice mail systems.
2. Video and voice call records must be managed in line with the Data Security Standard.

Monitoring and Privacy

1. Although Gamma does not carry out speculative investigations, Gamma reserves the right to monitor all use of Gamma Group resources. All investigations relate to policy violation or to protect Gamma from threat. a. Employees should not expect privacy by default when using the corporate network or company resources. Such use may include but is not limited to transmission and storage of files, data, and messages.

Web Proxy Usage Policy

To ensure a secure browsing environment and protect organisational resources from unauthorised access, malware, and other cyber threats, all internet traffic originating from organisational devices and systems must be routed through an authorised web proxy solution. This policy applies to all employees, contractors, vendors, and third parties using the organisation's network or accessing its resources.

1. Mandatory Use of Web Proxies
   a. All internet-bound traffic from organisational devices or systems must be routed through Gamma's authorised web proxy to enforce security controls, including content filtering, malware protection, data loss prevention (DLP), and adherence to regulatory requirements.
   b. Direct access to the internet that bypasses the web proxy is strictly prohibited.
2. Blocked and Monitored Content
   a. The web proxy will block access to unauthorised websites, including but not limited to those hosting inappropriate, illegal, or malicious content.
   b. User activities conducted through the web proxy are subject to monitoring and logging to ensure compliance with Gamma's security policies and regulatory obligations. Monitoring

activities will be performed in accordance with applicable data protection and privacy regulations, ensuring transparency and proportionality.

3. Configuration Compliance
    a. Users must not attempt to disable, bypass, or otherwise interfere with web proxy settings implemented on their devices. Such actions will be considered a violation of this policy and may result in disciplinary action.
    b. Personal devices connecting to the Gamma network must comply with web proxy controls, which may include the installation of organisational security software or configuration settings where applicable.
    c. Configuration changes to organisational systems and devices are strictly controlled and must follow Gamma's change management procedures.
4. Incident Response and Reporting
    a. Users encountering blocked websites or experiencing technical issues related to the web proxy must report the incident to the IT support team for resolution following Gamma's incident response protocols.
    b. Any attempts to bypass or tamper with web proxy controls will be logged, investigated, and handled in accordance with Gamma's incident management and disciplinary procedures.
5. Periodic Updates and Notifications
    a. Gamma reserves the right to update web proxy configurations to address emerging threats, comply with legal and regulatory changes, or enhance security measures.
    b. Users will be notified of significant changes to the web proxy policy or configuration through regular security awareness communications.
6. Enforcement and Acknowledgement
    a. Non-compliance with the web proxy usage policy may result in:
        i. Restricted access to organisational resources.
        ii. Disciplinary action up to and including termination of employment or contract.
        iii. Potential legal action in the event of intentional violations resulting in harm to the organisation.
    b. By using Gamma devices, networks, or accessing any Gamma systems, all users acknowledge and consent to the mandatory use of the web proxy and agree to adhere to this policy.
    c. Gamma will conduct periodic reviews and audits of web proxy configurations and associated logs to ensure compliance with security frameworks and legal obligations.

Responsibilities

Reporting of Security Incidents

If a security incident or breach of any security policies is discovered or suspected, the employee must immediately notify the IT Service Desk on 0333 240 3400.

    a. Outside of office hours, incidents must be reported to the on call IT Engineer on 0333 240 3400 providing details of the situation.

General security concerns or questions should be raised with the Group Security Operations Centre (security@gamma.co.uk).Examples of incidents that require notification include: a. Suspected compromise of login credentials (username, password, etc.).

b. Suspected virus/malware/Trojan infection.
c. Loss or theft of any device that contains company information.
d. Loss or theft of ID badge or key card.
e. Any attempt by any person to obtain a user's password over the telephone or by email.
f. Any other suspicious event that may impact Gamma's information security.
g. Employees must treat a suspected security incident as confidential information.
h. Employees must not withhold information relating to a security incident or interfere with an investigation.

1. The Group Network and Security Director is responsible for the content of this policy
2. People managers are responsible for their teams following this policy.
3. All employees are expected to adhere to the policy.

Policy Adoption

Violations of this policy will be managed through the Gamma Disciplinary process.