creative communications group

penguins GROSVENORCOMMS hlmlx FIREHOUSE a-vision

Supplier Handbook

ISMS DOC 125 (B)

Version:	ISMS DOC 125 (B)
Date of version:	06/06/2023
Created by:	James Hurley
Approved by:	Richard Parmenter (CISO)
Classification level:	Restricted
Next Review Date	06/06/2024

Change Log

Date	Version	Notes
06/06/2023	2.0	Second release

Introduction

Contained within this handbook are the **DRPG** company policies which are relevant to the product or services that you are providing to **DRPG**.

We vet our suppliers to ensure business practices mirror our own. This includes commitment to diversity and equal opportunities, health and safety, information security management, sustainability, environmental awareness, fair trade, FSC, anti-slavery, ethical marketing and bribery.

Please note, for the purposes of this guide, 'team members' includes all employees of **DRPG** as well as contractors, freelancers, temporary staff, apprentices, suppliers and third parties that are granted access to organizational information assets or systems.

Everything we do is based on **DRPG**'s guiding principles, sustainability objectives, and most of all, values:

- Understand the needs of everyone
- Passion for everything you do
- Trust in yourself every time
- Belief in everything you do
- Ownership to take charge of your own role and own your success

If you have any queries about the onboarding or vetting process then please email the Supply Chain Management Team at scm@drpgroup.com where we will be happy to assist.

Welcome.

Table of Contents

Information security

DRPG is committed to ensuring the highest levels of information security for our clients. We are committed to preserving the confidentiality, integrity and availability of all our information systems and client data throughout the organization. **DRPG** is certified to, and aligned with globally recognized information security standards, the ISO27001 and it is everyone's responsibility to maintain a culture of security.

DRPG's ISMS (Information Security Management System) is intended to be an enabling mechanism for information sharing, electronic operations and for reducing information-related risks to acceptable levels.

In particular, supplier management, business continuity and contingency plans, data backup procedures, avoidance of viruses, hackers and emerging cyber threats, access control to systems and information security incident reporting are fundamental to supporting the ISMS.

Please read the full information security policy at **drpgroup.com/suppliers**.

Contained within this handbook is key information that you will be required to adopt and work towards whilst engaging with **DRPG**. If you have any questions regarding information security, then please contact the Information Security Manager at ISM@drpgroup.com

Information classification guidelines

DRPG is an agile dynamic organisation with limited appetite or overhead for managing overly complex marking schemes. It does however recognize the importance of effective information classification to protect information and assets based on its value and importance.

We have conducted extensive risk assessments and consideration of assets as regards confidentiality, integrity and availability.

Please refer to the following policy for the appropriate classification, labelling and handling of **DRPG** information assets at **drpgroup.com/suppliers**.

Data Protection and Privacy

The significance of data protection and privacy cannot be overstated. **DRPG**, whether operating in the United Kingdom, the European Union, or the United States, Data Controllers and Data Processors must recognize and uphold the fundamental rights of data subjects. Safeguarding personal data is not only a legal obligation but also a moral imperative, ensuring trust, transparency, and respect in an increasingly data-driven world. By adhering to data protection regulations, businesses can foster a culture of responsible data handling, foster customer confidence, and mitigate the risks associated with unauthorized access, misuse, or exploitation of sensitive information.

DRPG have developed the following policy to set forth minimum requirements to ensure the protection of subject data, the Data Protection and Privacy security policy can be viewed at **drpgroup.com/suppliers**.

Information Security Incident Reporting

Reporting information security incidents is of the utmost importance. It plays a critical role in safeguarding organizations, individuals, and the overall integrity of data systems. Prompt and accurate reporting allows for swift action to be taken in response to security breaches, ensuring that appropriate measures can be implemented to mitigate the impact and prevent further harm. By reporting incidents, organizations can identify vulnerabilities and weaknesses in their systems, enabling them to address them effectively and enhance their overall security posture. Moreover, reporting incidents contributes to a collective knowledge base, allowing for the sharing of

information and best practices across industries, which ultimately strengthens the resilience of the broader cybersecurity ecosystem. Finally, reporting incidents is often a legal requirement, as many jurisdictions have established regulations that mandate the reporting of certain types of breaches.

Complying with these regulations not only helps organizations avoid potential penalties but also demonstrates a commitment to accountability and responsible data stewardship.

The purpose of this policy is to reduce the risk to assets, systems, and data and to ensure data to an affected system can be returned to an operational state as quickly as possible. All **DRPG** team members, and all owners of organizational information assets or systems are required to be aware of, and to follow this procedure in the event of an incident.

Please read the full information security policy at **drpgroup.com/suppliers**.

Health and safety policy

DRPG's health and safety policy shows our commitment to protecting our team members and others affected by our activities. As a responsible and conscientious organisation, we are committed to maintaining a healthy and safe working environment for everyone involved. Our Health and Safety Policy outlines our dedication to creating and upholding a culture of safety, managing risk, preventing accidents, and ensuring the welfare of all individuals associated with our operations.

For our full policy details visit **drpgroup.com/suppliers**.

H&S Incident reporting

All team members and all owners of organizational information assets or systems are required to be aware of and to follow this procedure for reporting any near misses or incidents.

- All health, safety, sustainability and environmental incidents and near-misses are to be reported to the H&S@drpgroup.com, or via phone to +44 (0) 1299 250531
- Minor incidents and requests can be logged via **DRPG**'s web-based software "The Surgery" if you have access
- Information security events and weaknesses can be reported to the IT Service Desk on +44 (0)1299 382060, or by email to support@drpgroup.com.

In certain circumstances, team members are not allowed to continue working after identifying a possible non-conformance, incident, weakness or information security event until given the express consent from the information security manager on ISMS incidents or from the health, safety, sustainability and environmental manager on other non-conformances. The process is as follows:

- The information security manager reports back, by email or phone, and will update the service desk ticket. In certain circumstances the line manager will be notified to describe how the event was dealt with and closed out
- The Service Desk ticket, together with the weakness/event report, and any documentation arising from the event and the response to it that has been generated will be logged and reported to the ISSG (Information Security Steering Group) for review.

Suppliers are expected to follow the above process and forward reports to the appropriate email addresses containing as much information

as possible immediately or as soon as practically possible.

This ensures we are compliant with our ISO standards, HASAWA, RIDDOR, Environment Act, and the UK/EU Data Protection Act (as well as any local laws and all other current regulations).

Sustainability policy

Here at **DRPG** we are dedicated to environmental stewardship, social responsibility, and long-term economic resilience. Our approach to sustainability extends beyond environmental considerations. We foster social responsibility by promoting diversity, equity, and inclusion. Our corporate social responsibility extends to building strong relationships with the communities we operate in, supporting local initiatives and charities. Check out our sustainable development policy.

For our full policy details please visit **drpgroup.com/suppliers**.

Anti-bribery policy

Integrity and ethical business practices are at the heart of everything we do. We are committed to maintaining the highest standards of honesty, transparency, and compliance with anti-bribery laws and regulations. **DRPG**'s Anti-Bribery Policy serves as our steadfast commitment to combatting bribery and corruption in all forms.

We firmly believe that bribery undermines fair competition, erodes trust, and damages the reputation of organizations. We are dedicated to conducting our business with integrity, ensuring that no form of bribery, whether direct or indirect, takes place within our organization or in our interactions with third parties.

It includes the Foreign Corrupt Practices Act (FCPA). It applies to all our business activities, both within the United States and internationally.

For our full policy details please visit **drpgroup.com/suppliers**.

Acceptable use policies

Use of these internet, email and systems provided by **DRPG**, to team members is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of the company.

DRPG's acceptable use policies aim to protect all equipment and data and minimize risk by providing clarity on the behaviors expected and required by team members. For our full policy details please visit **drpgroup.com/suppliers**.

If you are assigned a unique user ID or granted access to hardware or systems then the following will apply.

General

- **DRPG** user IDs, access to systems and email services may only be used for **DRPG** sanctioned communications and **DRPG** business related work
- Distribution of any information through the internet may be scrutinized and monitored by **DRPG**
- The use of **DRPG** computer resources is subject to local laws and regulations and must comply with UK/EU GDPR policies, where relevant.

Internet

- Team members may not visit internet sites on corporate issued devices that contain pornography, obscene, hateful, or other objectionable material, shall not attempt to bypass organizational web control technologies

and shall not make or post indecent remarks, proposals or materials on the internet or via social media

- Team members may not upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to the company or any third parties
- Team members may not download software from the internet or execute any software programs unless in accordance with **DRPG**'s software policies, and subject to authorization from the Service Desk.

Security

- Team members will uphold **DRPG**'s anti-malware/anti-virus policies, will not intentionally interfere in the normal operation of the network, and will not examine, change, or use another person's information assets without the owner's explicit permission
- Team members will not carry out any other inappropriate internet activity and will not waste time or resources on non-organization business.

Monitoring

- All **DRPG** resources, including computers, email and voicemail are provided for business purposes and may be subject to monitoring for security and network management
- **DRPG** does not routinely monitor email, internet traffic or other uses of IT, however monitoring software is constantly recording network activity and this system may be used to undertake spot checks.

Email

- Organizational email may not be used to defame, harass, make unauthorized purchases or publish views and opinions about team members, workers, suppliers, partners or clients of **DRPG**
- Users are prohibited from amending or deleting automatic email footers
- Email may only be used for the communication of confidential information as long as appropriate encryption methods have been applied
- Team members must not open incoming email attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party, were not expected – such emails must be reported to the IT Service Desk
- Team members are prohibited from using organizational email for forwarding chain letters, impersonating other people, and leaving on any websites other than for legitimate and necessary business purposes
- Team members are requested to limit the use of group email addresses
- Team members are required to comply with the Incident Reporting Procedure contained within this handbook
- All incoming and outgoing **DRPG** email is archived within GFI MailArchiver
- Team members are required to delete non-essential email messages as soon as possible and, on a regular basis, to clear email boxes of correspondence that is no longer required
- Organizational email may not be used to purchase anything on behalf of the **DRPG** without specific prior authorization
- Team members are prohibited from setting up automatic forwarding of emails to addresses external to that of **DRPG**.

Social media

- Team members are prohibited from revealing any **DRPG** confidential or proprietary information when engaged in blogging or social media
- Team members shall not engage in any blogging that may harm or tarnish the image,

reputation and/or goodwill of **DRPG** and/or any of its team members

- Team members may not attribute personal statements, opinions, or beliefs to **DRPG** when engaged in blogging or posting to social media
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, **DRPG**'s trademarks, logos and any other intellectual property may also not be used in connection with any blogging activity unless express permission has come from the **DRPG** Marketing department
- Team members are not to publish, post or release any information that is considered confidential or not classified as public
- Team members should get appropriate permission before referring to or posting images of current or former employees, members, vendors or suppliers
- When using **DRPG** computer systems, use of social media for business purposes is allowed, but personal use of social media networks is discouraged.

General Security

Passwords

- Usernames and passwords will be issued in line with **DRPG**'s procedures
- Team members will change their initial temporary password at first log on
- Team members will select and use passwords that are at least 12 characters in length, are alpha-numeric, are not based on any easily guessable or memorable data
- Team members will keep passwords secret, and will not store passwords in any automated log on process or browsers
- Passwords will be changed at intervals as required by **DRPG** – Currently 180 days
- Team members will not use the same password for organizational and personal use
- Team members must change their password in the event of any suspected breach.

Desks

- No confidential or restricted information (in paper or removable storage media format) is to be left on your desk
- Team members are required to ensure no one is able to access unattended workstations, and a password protected screensaver must operate within 10 minutes of inactivity
- Active computer sessions must be terminated by logging off when finished
- No personal storage media is to be used on **DRPG** systems
- Personal laptop devices are not to be used on the corporate network without express permission from the IT Service Desk
- Use of **DRPG**'s reproductive equipment (photocopiers, scanners) is for organizational purposes only.

Software

- No attempt to disable or over-ride any of **DRPG**'s pre-installed software may be made
- Team members are not to download or install any software of any sort without prior authorization of the IT Service Desk – this includes freeware, shareware, screensavers, toolbars etc
- MS Teams is the only permitted IM facility.

Data control and legislation

- Authorization is to be obtained from the asset owner for the storage of any **DRPG** personal information, client personal identifiable information or sensitive identifiable information
- All legal requirements in respect of computer use, including privacy and data protection regulations are to be abided by.

Backup and information classification

- Team members are responsible for ensuring all information on any workstation is correctly classified and labelled
- Team members are responsible for backing up, on the appropriate server, SharePoint site or within OneDrive, information on any portable device.

Maintenance

- Team members accept responsibility for the physical security of any devices and will report any damage/faults to support@drpggroup.com immediately.

Audit and security monitoring

- **DRPG** reserves the right to monitor all forms of communication to ensure that policies and procedures are being abided to
- All server access is recorded and monitored
- Requests for additional access to files/folders/servers must be forwarded to the appropriate line/project manager, who must put the request in writing and submit to support@drpgroup.com
- Access permissions will be recorded and maintained by the IT Service Desk and reviewed at least annually.

VPN

- It is the responsibility of team members with VPN privileges to ensure that unauthorized users are not allowed access to **DRPG** internal networks
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped
- VPN gateways will be set up and managed by **DRPG**
- All computers connected to **DRPG** internal networks via VPN must use the most up-to-date anti-virus software that is the corporate standard
- VPN users should disconnect from the network if being left unattended for more than 30 minutes
- Users non-**DRPG**-owned equipment must present their equipment to IT to ensure it complies with **DRPG**'s policies
- Only InfoSec-approved VPN clients may be used.

Mobile phones

If you are issued with a company mobile device, you must always observe the following rules.

General

- Only **DRPG** team members are permitted to use a company mobile device
- Team members must keep their mobile devices switched on, and on their person during working hours
- Company mobile devices are for **DRPG**-related activities only
- Personal calls should be limited to only those absolutely necessary
- You must not use any service of an improper, offensive, abusive, indecent or menacing nature on a company mobile phone
- Inappropriate or offensive material must not be uploaded, downloaded or stored on your company mobile device in any format
- The photographing or filming of fellow team members or any member of the public without their consent may breach an individual's right to privacy, so should be carefully considered.

Hardware and equipment

- The mobile device and any related equipment are the sole property of **DRPG**
- Team members are required to retain the box with all documentation and accessories if provided
- The company can demand the return of the mobile device or related equipment at any time

- **DRPG** does not provide or install hands free kits for vehicles, other than those owned by the company
- Any mobile device supplied with a protective case should be used.

Breakdown and repair

- In the event that your mobile device develops a fault, please contact **DRPG** Group Services
- All mobile devices are covered under warranty for mechanical failure for 24 months and are subject to a 24-hour faulty replacement
- Where a mobile device is damaged due to neglect or an act of purposeful destruction, all costs incurred in repairing or replacing the device will be your responsibility.

Security

- Team members are responsible for the security of their company mobile device and any information held on it
- Team members must ensure that mobile devices are not left unattended in either a public place or vehicle
- Should a company mobile phone or SIM card be lost, stolen or damaged, the team member must notify their line/project manager immediately so necessary measures can be taken to limit its use
- Where a mobile device has been lost or stolen due to the above details not being adhered to, the team member will be responsible for all costs incurred in gaining a replacement and settlement of any charges incurred.

Safety

- **DRPG** prioritizes safety and strictly prohibits the use of mobile phones while operating company-owned vehicles or conducting business-related tasks on the road – we adhere to local laws and regulations regarding mobile phone usage while driving.