Heardat (Pty) Ltd – Information Security Policy

February 2019 | Version 1.0

287 Fitzgerald street, Centurion, 0157
c: 082 222 6668 t: 012 653 3830 e: charl@heardat.net

Table of Contents

1. Introduction

This is the official policy for using our IT infrastructure in a way that is acceptable and responsible. The policy covers all IT infrastructure that we use. Any person who logs onto our network or uses our IT equipment or infrastructure must obey this policy. The information security requirements described in this policy are in line with national and international best practice for corporate organisations.

1.1. Why does this policy exist?

This policy exists because we need to protect personal information, and other kinds of information. We want to protect personal information to prevent real people from suffering real harm. When incidents occur, bad things can (and do) happen to ordinary people, including:

- **identity theft** – criminals can use stolen personal information to pretend to be another person, usually harming that person in the process;
- **discrimination** – anyone can use stolen personal information about someone to discriminate against them; or
- **embarrassment** – having private, personal information become public can be embarrassing.

Bad things can also happen to organisations, including:

- damage to our reputation;
- financial loss; or
- heavy demands to fix incidents.

1.2. How does this policy work?

We have invested in the best IT infrastructure and encourage you to use it for your own benefit and ours. We want you to use IT to do business, but we also want you to guard against the risks associated with it, especially risks to data protection and personal information. For clarity:

- **Personal information** means any information about an identifiable living human being or existing juristic person.
- **IT** means the combination of information, communications, and technology.

The purpose of this policy is to explain and describe:

- the risks associated with IT;
- how you must help us manage them; and
- the reasonable and appropriate technical and organisational measures that we use to secure the personal information that we are processing.

This policy is our high-level action plan for information security. We have identified the relevant legal requirements that may affect our information security and listed them in this policy, which we may update from time to time. This document is a policy and not a procedure. It tells you:

- why we need to protect personal information;
- how we expect you to help us protect personal information, at a high level;
- the minimum standards that both you and we must meet to protect the confidentiality, integrity, and availability of our information, communications channels, and technology; and

- acceptable ways to use our information, communications channels, and technology.

It does not tell you:

- exactly how to help us protect personal information; or
- the prescribed procedures when it comes to our information, communications channels, and technology.

2. Risks

Some risks associated with your use of IT include:

- **abuse** – our IT equipment and infrastructure could be compromised by abuse.
- **exploitation** – we have IT assets that are vulnerable to exploitation by third parties.
- **reputational damage** – we have a reputation that you could damage through your use of IT.
- **liability** – we could be held liable for what you do with IT as our employee, contractor or client.

3. Audience

3.1. Application

This policy applies to you if you are our:

- **employee** – if you have a permanent or temporary employment contract with us, as an ordinary employee, manager, or executive officer; or
- **contractor** – if you have an agreement with us to provide us with goods or services or do so on our behalf as a supplier, vendor, service provider, consultant, or any other kind of contractor.
- **client** – you have an agreement with us and we provide a service to you.

This policy applies to you when you use IT in any way, at any time, as allowed by relevant law, including when you use your:

- **IT equipment** – the necessary IT devices to do your work, including computers, printers, and any other hardware used for the IT infrastructure.
- **IT infrastructure** – the entire organised system of IT structures, facilities, and components necessary for the operation of our organisation, including data, computer networks, and software

This policy applies regardless of whether or not that IT equipment or infrastructure is:

- held on our premises or offsite;
- maintained or supported by our own personnel or third party contractors acting on our behalf; or
- owned by us or leased from someone else.

3.2. Acceptance

You must accept this policy as a condition for you to become our **employee**, **contractor** or **client**. You must adhere to this policy once you have accepted it. We may take disciplinary action against you if you violate it. Please ask us to explain it to you if any parts are unclear.

You accept this policy by:

- **doing so explicitly** – such as by checking a checkbox saying that you do, signing it, or agreeing to another document that incorporates it by reference, such as an employment or contractor agreement
- or **using our IT in any way** – such as by accessing any of our IT infrastructure with our authorisation using an authentication method, such as by entering your username and password or other credentials

3.3. Contact information

We may need to contact you with regarding this policy. Please make sure that your contact information is up to date in the relevant database. Please contact us if you are not sure what the relevant database is.

4. Acceptable standards

You may use IT to do business in any way, provided that it meets our acceptable standards of use, content, and conduct and is otherwise consistent with this policy.

4.1. Use

You may not use IT for any unacceptable purpose, including:

- **excessive personal use** – such as browsing the internet or social media to the detriment of your work during office hours, printing a significant number of personal documents, or any other uses that interfere with normal business activities; (applies to employees and contractors).
- **secondary business use** – such as running another business remotely, working for somebody else, or otherwise conducting any business not related to ours from our IT infrastructure or equipment;
- **inappropriate communication** – such as using your work email address for excessive personal correspondence, sending messages to someone without their permission, sending chain emails to your fellow employees or contractors, or excessive social chatting over instant messaging; (applies to employees and contractors)
- **deceitful communication** – such as attempting to access any communications addressed to someone else or creating messages so they appear to be from someone else;
- **personal software** – such as installing your own software on our IT infrastructure without our permission;
- **inappropriate credential use** – such as using your work email address, username, password, or similar identifying information to sign up for newsletters, web services, or public internet forums not related to your work (applies to employees and contractors); or
- **other unacceptable purposes** – any other purpose that adversely affects you, our employees or contractors, our business partners, or us.

4.2. Content

You may not use IT to publish any prohibited content including:

- **illegal content** that is prohibited by law – such as child pornography, pirated content, or content that otherwise infringes someone else's rights;
- **harmful content** that could cause harm to someone – such as defamatory comments, fraudulent claims, or untrue statements;
- **offensive content** that could reasonably offend someone – such as pornography, obscenities, or prejudicial or discriminatory statements; or
- **impermissible content** – such as content contrary to codes or standards to which we subscribe.

If you come across prohibited content, you should report it to us. We will either instruct you to delete it immediately or escalate it to the appropriate person.

4.3. Approval

Management must approve certain kinds of content before you publish it online, including if it is:

- **contentious** – such as political or religious statements;

- **potentially inflammatory** – such as swearing, foul language, or attitudes towards the sex lives and ethnicity of others;
- **about our products and services** – such as to advertise, promote, present, or otherwise make statements about them; or
- **otherwise concerning** – such as anything a reasonable person would be concerned about publishing because it may cause the public to view us negatively or bring us into disrepute.

Please ask us to review what you intend to publish if you are unsure whether or not it must be approved.

4.4. Conduct

You must conduct yourself acceptably, which means that you must:

- be **professional** – check your spelling, grammar, and punctuation;
- be **respectful** – do not be rude, threatening, harassing, bullying, hateful, racist, or sexist;
- be **honest** – do not lie or commit fraud;
- be **kind** – do not harass, or be hostile or disparaging towards others;
- respect **privacy** – do not unlawfully disclose personal information;
- respect **intellectual property rights** – do not commit copyright infringement;
- respect the **environment** – do not print documents or emails unnecessarily; and
- be consistent with the **spirit and intent of this policy** – be mindful of and act in accordance with the qualities highlighted, attitude put forward, and principles behind this policy.

4.5. Personal use

This policy does not unreasonably limit your ability to use IT in your personal life. But, what you do in your personal capacity can reflect on us as your employer or contracting party, if someone can identify you as working for us or being a client. This policy applies to your personal use of IT whenever you do anything that can be linked back to us. You are responsible for anything that you do with IT in your personal capacity.

5. Privacy

If you are involved with the design and development of business systems, you must consider and incorporate the following privacy principles into your work:

- **information security** – take all reasonable steps to protect information from misuse, keep it secure and make sure that others do the same;
- **data minimisation** – collect only the minimum amount of information necessary to accomplish a specified purpose;
- **transparency** – do not use information collected for any other purpose unless agreed with the data subject, authorized, or mandated by law;
- **accuracy** – maintain information collected in a sufficiently accurate, timely, and complete manner to protect the interests of the individuals and businesses; and
- **security** – implement adequate technical and organisational security measures to properly safeguard the collection, use, and maintenance of personal information.

6. Information

Information means the knowledge or facts that you learn or we provide to you about something or someone. You will likely handle personal, customer, business, confidential, and restricted information while working with us – each of which is subject to certain restrictions.

6.1. Types

You may come across various types of information while working with us, including:

- **personal information** – any information about a living human being or an existing company, close corporation, or other juristic person, provided that they are capable of being identified;
- **customer information** – related to anyone that we provide with goods or services, and includes account numbers (which are most important);
- **business information** – proprietary information regarding how we provide goods or services that we do not intend to disclose to third parties or the public;
- **confidential information** – that is only known to you through your employment, contractor or client relationship with us, and which you would not have known otherwise; or
- **restricted information** – that should only be known to authorised employees or contractors, which may not include you.

We may collect or generate personal, customer, business, confidential, or restricted information. This information is either our property or we have certain rights in it. We trust you to respect these rights, and to use the information to do your job as set out in this policy. We may monitor your use of the information and enforce the policy against you if you breach it, including taking disciplinary action against you.

6.2. Protection

You must protect any information we give you access to, by adhering to the following principles:

- **purpose limitation** – only using it for the purpose that we gave you access to it for;
- **permissible retention** – only retaining it for as long as is necessary for that purpose;
- **appropriate storage** – storing it appropriately;
- **business continuity** – creating any necessary backups, particularly of information on your company desktop or laptop (we do not usually backup information stored locally);
- **confidentiality** – not disclosing it to anyone that is not authorised to access it;
- **security** – securing it and not allowing anyone to access it if they are not authorised to do so;
- **isolation** – securely isolating any highly sensitive information systems that require extraordinary protection for business reasons.

In addition to the above, you must treat the following types of information in the following ways:

- **customer information** – you must process this lawfully in terms of relevant data protection laws;
- **business information** – you must not disclose this to anyone outside of our organization;
- **confidential information** – you may not disclose this to anyone we have not authorised you to;
- **restricted information** – you may not obtain, use or disclose this unless we authorise you to.

6.3. Confidential and restricted information

Confidential and restricted information is subject to the following additional requirements:

- **appropriate protection** – you must protect this information in a way that is appropriate to how sensitive or critical it is at all times, regardless of where or how it is stored, the systems or processes used to handle it, or the people who have access to it;
- **consistent protection** – you must protect this information consistently, regardless of where you are, including if you are at the office, working remotely, or at home;
- **no vulnerable disclosure** – you may not expose this information in public places where unauthorised people might discover or overhear it; and

- **no unauthorised disclosure** – you may not disclose this information without authorisation, even if it is not explicitly marked as confidential or restricted information.

6.4. Access restrictions

We may restrict your access to certain information using logical access controls. Please ask us for approval if you require access to additional information. We may restrict your access to that additional information according to your specific requirements.

6.5. Remote access

Remote access is the ability to connect to IT equipment or infrastructure from other IT equipment or infrastructure in another place, such as through a virtual private network, file synchronization software, or a web portal. Remote access is a security risk and we will only allow you to access our IT infrastructure remotely if:

- it is for legitimate business purposes; and
- you can show a business need.

6.5.1. Conditions

Your ability to access our IT infrastructure is subject to the following conditions:

- **provided solutions** – you must only use remote access solutions that we provide you with;
- **care and consideration** – you must treat your remote access connection with the same care and consideration as you would your on-site connection;
- **no concurrent connections** – you must ensure that your device which is remotely connected to your corporate network is not connected to any other network at the same time;
- **password confidentiality** – you may not share your remote access login password with anyone;
- **no network or data access by others** – you must ensure that no one else uses your device to access our network or any data relating to our business;
- **misuse or abuse your responsibility** – you are responsible for the consequences of someone misusing or abusing your remote access;
- **personal device** – you must ensure that your personal device is loaded with our approved and updated anti-virus software, and the latest operating system patches;
- **no home equipment reconfiguration** – you may not reconfigure your home equipment for the purpose of split tunnelling, dual-homing, or Frame Relaying when accessing our system;
- **prohibited conduct** – you may not do any form of network monitoring which will intercept data not intended for you, or port or security scanning with your remote access, unless it is a part of your ordinary job duties or you have otherwise gotten written approval from us; and
- **virtual private network** – you may only access our IT infrastructure through a VPN if we have approved your application and then only from approved devices.

6.6. Data breaches

If you know or suspect that a data breach has occurred, you must notify us by email as soon as possible. You must give us any information you may have that may help us limit the consequences of the breach, including a description of its cause and possible consequences, the identity of the unauthorized person, and any measures you recommend or have already taken.

6.7. Leaving our organisation

When your **employee**, **contractor** or **client** relationship with us comes to end, you must return to us all information that we gave you access to during the course of your relationship with us. You may not take any information out of our organization.

7. Communication

Communication means ways of sending, receiving, or exchanging information between people using some form of technology. We provide you with access to various communication channels, so that you can do business by communicating with our customers, our prospects, and your fellow employees or contractors. These channels have risks associated with them that you must guard against. The channels include:

- **internet** – a worldwide network of devices and the backbone for our other communication channels;
- **email** – a system for sending messages electronically through desktop or mobile mail to client linked to mail servers or webmail; and
- **social media** – various mass communications platforms including social and professional networking websites, video and photo sharing websites, blogs and micro-blogging websites, forums and discussion boards, and wiki websites.

You represent us whenever you transmit over a channel something that could be associated with us. You may not represent us contrary to the requirements of this policy.

7.1. Internet

You may use the internet to do business and for reasonable personal use. However, we may put in place certain controls to monitor, filter or otherwise regulate your use of the internet. When using the internet:

- **personal use** – you may only make reasonable personal use of the internet incidental to your business use, provided that you must use your good judgement to determine what is reasonable and you do not disrupt the internet, expose us to a marked increase in cost, interfere with your own or anyone else's daily work activities, or break the law;
- **unacceptable content** – you may not use the internet to access offensive or disruptive content, such as political statements, inflammatory religious statements, profanity, statements viewed as harassing, racist, defamatory, or sexually explicit, implicit, or connotative, or any other content that a reasonable person would deem unacceptable or offensive to someone else's age, race, sexual orientation, religious or political beliefs, national origin, or disability; (applies to employees and contractors)
- **unacceptable conduct** – you may not use the internet for any unacceptable conduct, including abuse, discrimination, defamation, or harassment;
- **respect intellectual property rights** – you must make sure that you are not infringing on anyone's copyright, database rights, trademarks, or other intellectual property rights by downloading files from the internet;
- **visit undesirable websites** – you many not visit any websites involved in distributing pornography, online dating, audio streaming, hacking, gambling, webmail services, file hosting services, or anything similarly undesirable; (applies to employees and contractors)
- **access the internet unofficially** – you may not use your own modem or other method of accessing the internet while connected to our IT infrastructure and may only access the internet though the network connections that we have approved;
- **make browser changes** – you may not make any configuration changes to the settings of your browser software or load any other browser type software on our IT infrastructure, because we have special rules governing all browser configurations;
- **use an alternative browser** – you may generally only use Google Chrome as your browser software, but you may use alternative browser software if you are the type of employee, contractor or client who needs to use alternative browser software in line with your job functions, such as software development, digital marketing, or other internet-focused activities;
- **have concurrent connections** – you may not connect to the local area network and mobile internet at the same time;

- **unsecured communication** – you may not communicate our confidential or sensitive information across the internet unless: it is encrypted, we have authorised the recipient, and you have authenticated their identity;
- **no bypassing safeguards** – you may not download information through instant messaging or chat mechanisms because they could bypass our internet safeguards.
- **unauthorised entry** – you may not use our equipment to make or attempt unauthorised entry to any network or computer accessible via the internet;
- **third party tunnelling** – you may not use third party services to tunnel other protocols or access internet applications via allowed ports or services, such as tunnelling POP3 through HTTP;
- **proxy mechanisms** – you may not configure local workstations to act as proxy mechanisms to grant internet resource access to other users who would not have had access to these resources under normal circumstances;
- **online privacy** – you must be careful with your personal or otherwise sensitive information online and must not give it to anyone that you do not trust;
- **online security** – you must do your best to only submit sensitive information through a secure internet connection where the website URL in your browser starts with 'https' (instead of 'http') and a small padlock symbol appears (you can usually click on or near the symbol to check that the website has a valid non-expired certificate, some browsers will also tell you whether a website has an expired certificate);
- **downloads** – you must be careful when downloading anything from the internet and make sure that you only download from reputable websites, because files from unknown sources may contain viruses, trojan horses, or other malware;
- **bandwidth** – you must be conservative with our bandwidth, because South Africa is a country with expensive internet infrastructure by international standards.

7.2. Email (only applies to employees and contractors)

We provide you with an email address and want you to use it to do business, but:

- **personal use** – you may only make reasonable personal use of the email facilities that we provide you with incidental to your business use, provided that you must use your good judgement to determine what is reasonable and you do not: disrupt our email facilities; expose us to a marked increase in cost; interfere with your own or anyone else's daily work activities; or break the law;
- **unacceptable content** – you may not send electronic communication messages containing any offensive or disruptive content, such as political statements, inflammatory religious statements, profanity, statements viewed as harassing, racist, sexual (explicit, implicit, or connotative) or defamatory, or any other content that a reasonable person would deem unacceptable or offensive to someone else's age, race, sexual orientation, religious or political beliefs, national origin, or disability;
- **identification** – you must make sure that your email identifies you to its recipient with your full name and not just your email address;
- **no falsification of origin or route** – you may not falsify email addresses, headers, or routing information so as to obscure the origins or route of a message;
- **disclaimers** – we automatically append our standard email disclaimer to all outgoing emails, you may not remove or tamper with it for any reason, and you must make sure that your email contains all links to our other relevant disclaimers as communicated to you in writing from time to time;
- **signatures** – you must be aware that an email from you to someone could constitute your electronic signature or consent if the contents of the message indicates a willingness to be bound, so be careful what you say in your emails;
- **unsolicited messages** – you must make sure that your messages are not unsolicited or the recipient may consider them to be spam;

- **bulk sending** – you must make sure that any bulk emails you send comply with the requirements of the relevant direct marketing laws and remember that BCC (Blind Carbon Copy) is the only option when you want to send a message to lots of other people while protecting the identity of the other recipients, so make sure that you understand when you should and should not use CC (Carbon Copy);
- **printing** – paper is inefficient, it kills trees, and costs our organisation money, so please do not print unless you really need to;
- **contents** – please do not alter the contents of the original email when you forward it or reply unless absolutely necessary, in which case you should mark the changes clearly;
- **file size** – please do not send emails or attachments that are too large, because we may need to filter emails by attachment size to conserve bandwidth and limit the size of mailboxes to conserve storage space (you should use alternatives to send large files, such as transferring them via secure FTP);
- **retention** – we will establish data retention rules for emails appropriate to the legal and business requirements of each specific business area, but you must avoid the unnecessary retention of emails in terms of those rules and make every reasonable attempt to reduce the volume of emails retained on the relevant email facility;
- **deletions** – however, please do not delete any emails or attachments if there is any chance that the organisation may require them later;
- **unstructured data** – you may not save .pst or any other mail archive files to any network share, external storage medium, or any other storage location other than your own hard drive;
- **spam** – you may not open, click on any links in, or reply to unsolicited emails and must delete them immediately when you receive them;
- **forwarding** – you may not forward chain emails, hoaxes (including Ponzi or other pyramid schemes), or virus warnings from other employees or contractors or anyone else;
- **solicitation** – you may not influence, persuade, or otherwise solicit others in regard to commercial ventures, religious or political causes, outside organizations, criminal activity, or any purposes not related to our business;
- **no personal email for work** – you may not use your personal email, webmail, or other non-company email account to send our confidential or sensitive corporate information, documents, or other work related content;
- **external forwarding rules** – you may not create forwarding rules to automatically route your internal work email to your personal or another external email address so that you can work remotely (however, you may contact us for approval and assistance if there is a valid business reason for automatic forwarding – pending a risk analysis);
- **email backups** – we archive all incoming and outgoing emails so that we can retrieve them later;
- **blocking** – we scan and will automatically block all incoming and outgoing emails containing or suspected to contain viruses, worms, or other malware as well as emails categorized as spam (no matter how important they are), although we may decide to review the block and release them if no malware is present and they are not actually spam;
- **file formats** – you may not send any audio files (such as wav, aiff, mp3, ogg, wma, or flac files), video files (such as avi, flv, wmv, mp4, or mov files), or executable files (such as apk, bat, bin, cgi, pl, com, exe, gadget, jar, py, wsf, or cmd files) as attachments because of the danger of them containing malware and we will block any attempts to do so;
- **report malware warnings or popups** – you must report malware warnings or popups that result from incoming email or attached file downloads to us immediately;
- **copyrighted materials** – you may not send or receive copyrighted materials which we do not own or otherwise have sufficient rights to distribute in that way;
- **off-boarding** – we will forward your email to a responsible party for a period of no longer than 90 days when you no longer work for us;
- **check recipients** – you must check email recipients before sending, forwarding, or replying to messages;

- **distribution lists and groups** – you may only use distribution lists and groups for valid business purposes, must consider whether or not each group member really needs to receive the email when using distribution lists, and you may not email them marketing material or other personal messages;
- **unauthorised communication** – you may not email our trade secrets, proprietary financial information, sensitive client or employee information, or similar materials to third parties without prior authorization from us;
- **contractors require approval for email** – you may not use an email address as a contractor at our organisation unless you have applied for special approval and we have granted you that approval in writing;
- **contractors email restricted** – if we grant you approval to use an email at our organisation, we may restrict that email to specific testing or limit its duration.

7.3. Social media

Your constitutional rights to privacy and free speech protect any online activity you conduct on your personal social networks outside the workplace with your personal email address which is not related to us. We will only grant you access to social media if you require it for regular business purposes. If you do, we encourage you to use social media to do business – but subject to the following conditions:

- **unacceptable content** – you may not post any content that is obscene, defamatory, profane, libelous, threatening, harassing, abusive hateful, or embarrassing to someone else, including comments about our employees, us, yourself, or our competitors;
- **infringing content** – you may not post any material or content that infringes on other peoples' privacy, publicity rights, or copyright;
- **identification** – you must identify yourself with your name and role within our organisation whenever you publish anything that could be connected to us;
- **no disclosure of our organisation or use of our logo** – you may not disclose the name of our organisation as your employer or contractor or use our logo on your private profile on informal social media platforms, however you may disclose our name as your employer on professional networking sites, such as LinkedIn;
- **distance your opinion from ours** – you must state that your opinion is yours and does not necessarily represent ours if you have listed us as your employer on a professional network and are expressing your personal view about a topic;
- **no dual accounts** – you may not use the same social media accounts for professional and private activities and you must use separate social network accounts if you use social media for both professional and private activities;
- **no agency to post about work** – you may not post about work-related matters and may not publish anything purporting to be our opinion or published on our behalf without our written permission;
- **no representation on our behalf** – the mere fact that you work for us does not imply that we have authorised you to speak as our representative and you may not use social media to conduct business activities on our behalf unless we have duly authorized you to do so;
- **our intellectual property** – anything that you publish on social media may not contain your work email address with us, our logos, trademarks, or anything else that could make it look as if we have endorsed what you have published, unless we have given you written permission to do so;
- **sensitivity and confidentiality** – you must only publish content on social media that consists of publicly available information and does not disclose any sensitive or confidential information that you only know because you work for us and you may never post any of our sensitive or confidential information on the internet or any sensitive information about our employees, contractors, or vendors;

- **references** – you may not refer to our customers or suppliers in anything that you post on social media without their permission;
- **veracity** – you must only publish content on social media that contains true and accurate information and you may not publish content on behalf of someone else or that someone else has prepared, because it is difficult to verify its accuracy;
- **attribution** – you must link back to the source of your statements whenever possible
- **work discussion groups** – you may only take part in work related electronic discussion groups if we have authorised you to do so;
- **non-work discussion groups** – you may not participate in non-work discussion groups and general entertainment media;
- **comply with our policy** – you must abide by our social and online media policy if we have authorised you to use social media to conduct business activities on our behalf;
- **comply with other policies** – anything that you publish on social media must comply with the relevant social media service's legal terms and any relevant copyright and other laws;
- **reasonable use** – social media is time-consuming, and you should keep usage to acceptable and reasonable timeframes, including lunchtimes and before and after office hours;
- **credential use** – you may not use passwords that you use at the office on social media websites or the internet in general;
- **disreputable activities** – you may not engage in any activities on social media which could bring us into disrepute;
- **you are responsible** – we will hold you responsible when using our email address or assets to engage in any social media activities, because most actions are typically public or at least semi-public;
- **our removal** – we may remove posts to our official website, social media community, or blog if the posts are defamatory, discriminatory, obscene, unlawful, inaccurate, untrue, or otherwise offensive;
- **your removal** – you must remove anything that you have published on social media that can be linked back to us if we inform you in writing that it is contrary to this policy.

7.4. Account security

We provide you with various credentials in the form of usernames and passwords to access various system accounts. These credentials pose security risks to us if you do not look after them. There is no such thing as absolute security, but there are various steps you can take to improve security. For this reason, please take the following account security steps:

- **username and password** – we will allocate you a unique username and password if you are to have access to our system accounts as an employee, contractor, or temporary staff;
- **password allocation** – you may formally request the initial allocation of a password from us, if we have not allocated one to you automatically;
- **password request** – you must formally request the resetting of an existing password from us through a formal process, subject to authentication and approval;
- **access controls** – please respect credentials and other access controls, because they are there to make sure that only authorised employees and contractors have access to our communications channels necessary to do their jobs;
- **password confidentiality** – your passwords are for your use only and you may not share your password for any system account with anyone else;
- **credential responsibility** – we will hold you responsible for all actions under your credentials, whether you shared your password with someone else or even if someone obtained it without your permission;
- **password exclusivity** – you may not use another person's username, password, or other credentials, unless we have given you specific written permission to do so;

- **exceptional password access** – we may formally grant you certain rights and privileges under certain circumstances, such as granting a secretary the rights and privileges to act on behalf of a manager (the more senior employee must arrange access via the delegation process in accordance with the approved procedures);
- **password storage** – you may not write down your passwords or store them electronically without adequate protection;
- **password strength** – you must use a sufficiently strong password consistent with the security standards of system that you are accessing so that it is difficult to guess;
- **password guidelines** – your password should conform with the following guidelines as far as possible (which we will enforce electronically on applications where possible): 8 characters' minimum length; 42 days' maximum age; composed of alphanumeric characters or combination of upper- and lower-case letters; and not contain easily guessable or identifiable words (such as family names or phone numbers);
- **regular password changes** – you must change your password regularly from time to time to reduce the chances of someone else knowing it;
- **exceptional password changes** – you must change your password immediately if you have disclosed it to support personnel, have disclosed it to another user, or suspect that someone else knows it;
- **password management** – you must not store your password so that others can find it, for example on paper or in an electronic file on your device;
- **log out** – you must log out of systems that you have logged into using your credentials whenever your equipment is unattended;
- **no generic usernames** – you may not use generic usernames, such as 'Sales1' or 'Sales2' unless a system requires it specifically;
- **no insecure password transmission** – you may not send permanent passwords through email, instant messaging, other electronic communications, or another insecure communication channel, such as leaving them on voicemails;
- **identification** – you may not misrepresent, obscure, suppress, or replace anyone else's identity on our IT infrastructure;
- **remember password** – you may not use the remember password feature on any application.

7.5. Password controls

We must make sure that all production system-level passwords are part of the global password management database managed by IT.

7.6. Mobile internet access facility (applies to employees and contractors)

We may provide you with a mobile internet access facility, such as a 3G or 4G connection on a device or through a dongle, router, or cell phone. This facility is strictly for business purposes and we may subject you to disciplinary action if you abuse it. You may only use mobile internet access facilities that we provide you with.

8. Technology

Technology means the equipment and infrastructure you apply to information for practical purposes. IT equipment includes both company devices that we provide to you and personal devices that you provide yourself. You may use IT equipment to access our IT infrastructure, provided that you comply with certain requirements.

8.1. Company devices (applies to employees and contractors)

We do not provide you with IT equipment in the form of company devices that you may use to access our IT infrastructure. A company device is any electronic device that we own or rent and let you use to do business and includes:

- both fixed devices, such as desktop computers or servers, and portable devices, such as laptops, tablets, and mobile phones;
- both the hardware and software on those devices;
- both the onsite and offsite use of the devices.

8.2. Personal devices

You may provide your own IT equipment in the form of personal devices used to access our IT infrastructure. A personal device is any electronic device that we do not own or are not renting from a third party that you use for the purpose of doing business. Personal devices include any kind of:

- **computer** – such as a desktop, laptop, tablet, or smartphone;
- **communications device** – such as a cell phone, modem, or mobile data card;
- **removable storage device** – such as a memory stick, external hard drive, or SD card; or
- **other storage media** – such as an optical or magnetic disk.

8.3. IT infrastructure

IT infrastructure is anything that provides you with access to information or communication channels and includes:

- **information resources** – such as servers, network attached storage devices, or server-based applications;
- **communication devices** – such as routers, switches, or modems;
- **connections** between those devices – such as network cables or wireless networks; and
- **peripheral** devices – such as printers, scanners, or copiers.

8.4. Device protection

You should take the following precautionary steps to protect your company and personal devices:

- **safeguarding** – take reasonable steps to protect them from physical damage and theft;
- **password security** – do not store any passwords or other credentials anywhere on the device (physically or digitally), including taping notes to the device itself or keeping notes inside the carry case of the device;
- **data security** – make sure that you protect and secure the data and software stored on it;
- **environmental protection** – do not leave the device in direct sunlight or where it is exposed to any other environmental hazards;
- **cleaning** – use a dust cloth and specialist cleaning products instead of household chemicals or water to clean the device;
- **physical protection** – do not drop or knock the device and check the condition of its carrying case regularly.

8.5. General device requirements

The following requirements apply to both company and personal devices:

- **theft or loss reporting** – you must immediately report the theft of any device to your line manager (if you are an employee) or contact person (if you are a contractor or client) as soon as possible in terms of the relevant procedure communicated to you in writing from time to time so that we can suspend all access to it, wipe it remotely if necessary, or instruct you to report the theft to the police;
- **device identification** – you must identify your device and carry case correctly by physically writing your contact details on it;

- **backups your responsibility** – we are not responsible for backing up or restoring your personal information and you must regularly copy all information stored on your workstations to designated information systems for backup and archiving purposes, because we do not generally backup information on desktops and laptops automatically;
- **backups methods** – you should generally only back up information to our servers, but you may backup information to your company or personal device if absolutely necessary provided that it is only a temporary measure and that you backup to our servers as soon as possible afterwards;
- **remote lock** – we may need to be able to lock your device remotely to prevent or thwart unauthorised access and we are allowed to install special software on it to do this;
- **data wipe** – we may need to be able to wipe your device remotely for security reasons or to prevent information from falling into the wrong hands;
- **special software** – we may install special software on your device to lock or data wipe it remotely.

8.6. Company device requirements

The following requirements apply to company devices:

- **responsible for access** – you must control access to any company devices that we have issued to you to prevent unauthorised access to the data on them or theft of the devices themselves;
- **business use** – you must use company devices primarily for business purposes and you may only use them reasonably for personal purposes;
- **safeguarding** – you must secure your laptop with a security cable when using it at the office;
- **locking** – you must manually lock your company desktop computers or laptops when you leave them unattended and not rely on any automatic lockout mechanism to prevent unauthorised access;
- **protection** – you must always run up-to-date anti-virus software on your company desktop computers or laptops, may not tamper with or disable it for any reason, and must immediately contact our helpdesk if you suspect that it is absent or faulty;
- **software** – you should only have software that we have provided you with installed on company devices and you may not install unlicensed software, privately owned software, or any other electronic media on company devices that is in breach of legislation or this policy;
- **authorised use** – we only authorise certain people to use company devices and you may not let anyone else use them, such as family members, unauthorised co-workers, or anyone else;
- **repairs** – you may not open the casing of any company devices for any reason and must instead hand the relevant device over to an authorised technician for repairs.

8.6.1. Company workstation requirements

A workstation is any desktop or laptop computer that we have assigned to you specifically for exclusive business use. The following requirements apply to them:

- **log off** – you must log off from your company workstation when you go home for the day or otherwise leave the premises;
- **password lock** – you must password lock your company workstation whenever you leave it unattended to make sure that nobody obtains unauthorised access by enabling a password protected lockdown screensaver set not to exceed 10 minutes of idle time;
- **remote takeover** – you must never leave your workstation unattended should an IT support analyst or engineer work on it via remote takeover and you may cancel the remote takeover at any time if you have concerns about the access.

8.6.2. Company laptop requirements

A laptop generally includes any portable computer that is small enough to rest on the user's lap, has a screen that closes over the keyboard like a lid so that it is flat when closed (although there are other configurations), or is suitable for use while travelling because of its small size and the fact that it is powered by a battery. The following requirements apply to them:

- **encryption** – you must have hard drive encryption software installed on them;
- **do not leave unattended and unsecured** – you may not leave your laptop unattended without: (i) locking it securely to an immovable object, locking it in a secured room, or taking other steps to secure it against theft; and (ii) securing it against unauthorised electronic access by making sure that it is password protected and logging out of it.

8.6.3. Company mass storage device requirements

Mass storage devices include USB memory sticks, memory cards, and external hard drives. The following requirements apply to them:

- **use** – you may only use encrypted memory sticks that we have issued you with to store business information and for all other business purposes;
- **restrictions** – you may not use any other mass storage devices to store that information.

8.6.4. Company IT facilities requirements

IT facilities are a combination of any premises, equipment, or amenities that we use for the purposes of IT, such as data centres, decentralised server rooms, or other IT facilities. The following requirements apply to them:

- **restricted access** – you may not generally access company IT facilities, unless we have given you specific written permission to do so based on a valid reason for requiring access;
- **video surveillance** – you may be subject to monitoring at our IT facilities by continuous observation of premises, particularly of entrances and exits, using CCTV or another video surveillance system to prevent unauthorised access to information and theft of our equipment.

8.6.5. Smart device requirements

Smart devices include mobile phones and tablets. The following requirements apply to them:

- **connection** – you may only connect to our IT infrastructure using the mobile content management solution that we have approved;
- **download only trusted applications** – you may only download 'apps' from trusted sources, such as marketplaces that have positive reviews and feedback.

8.7. Mobile device requirements

A mobile device is any device that you regularly carry about on your person and move from one place to another, whether a personal or company device – such as a smartphone, tablet computer, or laptop computer. The following requirements apply to them:

- **common threats** – you must safeguard mobile devices against common threats, such as password theft; malware (including viruses and worms); data corruption; data theft through line sniffing; theft of the mobile device itself; mobile code vulnerabilities; and wireless vulnerabilities;
- **anti-virus and updates** – you should install the latest anti-virus software on the device where applicable and update it regularly with the relevant patches;
- **backups** – you must back up data on the device regularly where possible, such as on a daily basis from your laptop computer where we provide you with a mobile device backup solution for that purpose.

8.8. Bluetooth device requirements

Bluetooth is a standard for connecting mobile phones, computers, and other electronic devices wirelessly at short range. The following requirements apply to its use:

- **turned off** – make sure that your Bluetooth functionality on your device is always turned off when not required;
- **non-discoverable** – make sure that your device is in non-discoverable mode when your Bluetooth functionality is turned on;
- **pairing password** – make sure that you use a strong password that is hard to discover when setting up Bluetooth pairing;
- **Bluetooth kits** – be aware of the security risks inherent in hands-free Bluetooth kits, because they do not have built-in software to authenticate other devices properly with a strong security key and are very easy to hack.

8.9. Personal device requirements

You may use your personal devices to access our IT infrastructure, provided that you meet the following requirements:

- **connection permission** – you have permission from us to connect your personal device to our IT infrastructure;
- **password protection** – you enable passwords to access the operating system or login from the screensaver or lock screen;
- **encryption** – you enable device encryption of all information in the operating system or other application whenever possible;
- **unauthorised use** – you do not let any unauthorised users use the device under any circumstances, including lending the device to an unauthorised user;
- **secure communications** – you use the necessary security software to establish a secure communication connection to our system when connecting to our IT infrastructure from off of our premises;
- **company software** – you let us load software onto your personal device before you access our IT infrastructure so that we can manage all devices centrally and enforce certain security measures on them, such as remote locking and data wiping;
- **standards** – your personal device meets certain standards in terms of operating system before we allow it to access our IT infrastructure, which we will provide to you on request;
- **protection** – your device has sufficient anti-virus and anti-malware software installed before we allow it to access our IT infrastructure or the internet through that infrastructure;
- **configuration** – your device is configured in a standard way, which may mean that we may not allow certain non-standard configurations or software such as unlocked or so-called ‘jailbroken’ devices.

8.10. Travelling risks

Please be aware of the following risks when travelling with your company or personal device:

- **public networks** – when connecting to public networks, such as Wi-Fi hot-spots, make sure that your anti-virus software is up-to-date and firewall program is running, because there are various risks associated with public networks that these will help minimise them;
- **reading screens** – watch out for ‘shoulder surfers’ and do your best to prevent others from being able to see what is on your screen when travelling on aircraft, public transport, or sitting in public areas;
- **hand luggage** – reduce the chance of a device being damaged or stolen by keeping it in your hand luggage instead of checking it into the hold when travelling by aircraft;

- **accommodation security** – make sure that the device is locked away securely in a safe or other secure area when staying in accommodation such as a hotel or guest house and not left exposed in your room, even if your room is locked;
- **storage in vehicle** – store your device securely out of sight in the boot or trunk when storing it in your vehicle and not on the back seat.

8.11. IT infrastructure requirements

The following requirements apply to IT infrastructure:

- **network share** – you must store all corporate information on your designated network share and may not create your own network shares;
- **no personal files** – you may not save personal files such as pictures, audio, or videos on any network share.

8.12. Software

There are certain software licensing rules that you must comply with in our organisation:

- **compliance** – you must use any software in compliance with its licenses and any applicable agreements;
- **installation** – you may generally only install business approved software on any company device and may not install any other software without checking with your line manager (in the case of an employee) or contact person (in the case of a contractor) that it is properly licensed or logging a call at the IT service desk and getting our approval;
- **downloaded software** – you may not install software downloaded from the internet without permission from your line manager (in the case of an employee) or contact person (in the case of a contractor);
- **unlicensed software** – you may not install any software for which we do not have a license or a sufficient number of licenses for the number of users that want or need to use it;
- **copyright protection** – you may not distribute copyrighted software without the legal right to do so
- **copying software** – copying software will often infringe copyright protection and you may not do so without our approval;
- **no intellectual property infringement** – you may not otherwise infringe license agreements, copyright, patent, trademarks, or any other kind of intellectual property by installing or distributing ‘pirated’ software that is not appropriately licensed to us;
- **no circumvention software** – you may not download, install, or copy any software specifically designed to circumvent any existing security mechanism or features.

8.13. Malicious software

Malicious software includes programs such as viruses, trojan horses, and spyware that are meant to disrupt and damage IT. They pose significant risk to us and constantly threaten the confidentiality, integrity, and availability of our IT equipment and infrastructure. We need you to help us protect against these threats by:

- **no introduction** – not introducing any malicious software to our IT equipment or infrastructure for any reason;
- **avoid mass storage** – avoiding the use of mass storage devices, because they often propagate malicious software;
- **phishing or social engineering** – avoiding clicking on links, opening attachments in spam, junk or chain emails, and other kinds of phishing or social engineering attacks;

- **anti-virus software** – activating anti-virus software, updating it regularly, making sure that it stays active, and not interfering with any anti-virus software that we have installed on your devices to detect and eradicate these events;
- **updates** – updating operating systems and other critical software with security and related patches regularly;
- **suspicious sources** – not running software from unknown or disreputable sources;
- **report to IT service desk** – reporting it to the IT service desk as soon as reasonably possible if you suspect that your device is infected with malicious software by logging an incident or phoning the 24-hour support number;
- **care and precautions** – otherwise take the necessary care and precautions to prevent malicious software from being released on to our IT equipment and infrastructure.

8.14. Information security

We need you to help us protect any IT equipment or infrastructure from physical loss or damage through the following information security practices:

- **take care** – taking care of any IT equipment assigned to you;
- **store securely** – making sure that all data is stored securely, which means using electronic security measures in the case of data stored electronically and physical security measures in the case of data stored on physical security media;
- **no unauthorised significant changes** – not making significant changes to IT equipment or infrastructure without permission from your line manager (in the case of an employee) or contact person (in the case of a contractor);
- **no unauthorised removal of equipment** – not removing any IT equipment from our premises without our permission (applies to employees and contractors);
- **no unauthorised connection of equipment** – not connecting any unauthorised IT equipment to our IT infrastructure without our permission;
- **no duplicate storage** – not storing multiple versions of the same file unnecessarily;
- **no unauthorised access to infrastructure** – not granting unauthorised users access to our IT infrastructure;
- **report security incidents** – reporting security incidents to us timeously so that we can take appropriate action;
- **assist with restoration** – making yourself available and assisting, to the best of your abilities, with the restoration of normal business activity after an emergency or a disaster disrupts it.

8.15. Prohibited insecure conduct

You may not use IT equipment or infrastructure to do anything that would threaten our security or that of another system, including:

- **inappropriate access** – you may not access our information and information systems in a way that does not conform to your job function and description;
- **unauthorized access** – you may not access or use any system without permission, including attempting to probe, scan, or test the vulnerability of a system or to breach any security or authentication measures used by a system;
- **interception** – you may not monitor any data on a system without permission, unless it is part of your job description;
- **monitoring or crawling** – you may not monitor or crawl a system in a way that impairs or disrupts the system being monitored or crawled, unless it is part of your job description;
- **falsification of origin** – you may not forge TCP-IP packet headers, e-mail headers, or any part of a message describing its route or origin;
- **denial of service** – you may not inundate a target with communication requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective;

- **intentional interference** – you may not interfere with the proper functioning of any system, including deliberately attempting to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques;
- **operation of certain network services** – you many not operate network services such as open proxies, open mail relays, or open recursive domain name servers;
- **avoiding system restrictions** – you may not use manual or electronic means to avoid any use limitations placed on a system, such as access and storage restrictions.

8.16. Reasons for interception

We may monitor and intercept electronic communications for internal policy compliance, suspected criminal activity, lack of employee productivity and other systems management reasons in line with relevant processes.

9. General

While we respect your right to decide how to do business within our organisation, there will always be certain organisation-wide policies that we will require everyone to comply with so that our organisation can run effectively. You must comply with all aspects of this policy.

9.1. Monitoring

We may monitor your use of our IT infrastructure to ensure compliance, including email, messages and network connections. You consent to us monitoring your conduct in this way when you agree to be our employee or contractor, and when you log onto or otherwise access our IT infrastructure. All messages and information that you send through our IT equipment or infrastructure are our property, to the extent allowed by applicable law. We may also disclose their contents to law enforcement agencies, where necessary.

We may also monitor, access, retrieve, read, or disclose your communications at any time when:

- a legitimate business need for the action exists; or
- you are unavailable and timing is critical to a business activity;

provided that:

- you have given us prior consent for the action;
- there is reasonable cause to suspect criminal activity or material violation of our policies; or
- legal regulation or a third party agreement requires us to monitor you.

9.2. Limited right to privacy

We will respect your right to privacy to the greatest possible extent, but your right to privacy is limited in the interests of the business and we have the right to monitor you, which includes the rights to:

- monitor all internet traffic passing through our IT infrastructure;
- monitor any emails or other communications passing through our IT infrastructure; and
- access any file stored on our IT equipment or infrastructure;

provided that it is performed by our properly authorised representative for any lawful purpose strictly in accordance with any monitoring policy and procedures that we may have, including for the purposes of:

- checking internal compliance with our policies;
- investigating suspected criminal or otherwise unlawful activity; or
- other systems management reasons.

9.3. Limited private use

You are allowed to use our IT equipment and infrastructure for limited private use for private email correspondence and web browsing unrelated to our business to the extent that the use:

- conforms strictly to the restrictions contained in this policy;
- does not adversely impact on your responsibilities and duties towards us, including your productivity and working hours;
- does not adversely affect our IT equipment and infrastructure, including available bandwidth, storage space, and general operating capacity.

9.4. Blocking

We may block and delete any information passing through our IT infrastructure in our absolute discretion. We also reserve the right to block any type of information that is deemed not to be in the best interests of our business or existing policies.

9.5. Breach and enforcement

We may enforce this policy by taking appropriate disciplinary action against you if you breach it in any way. That disciplinary action will be in line with our disciplinary procedures policy, which may lead to serious sanctions, such as your dismissal or referral to the authorities for legal or criminal proceedings. We will review each breach of this policy on a case-by-case basis, but there is an onus on us to apply discipline consistently in the workplace in line with the relevant policies. Please refer to the disciplinary procedures policy to understand what the appropriate sanction could be for a breach of this policy. We may sanction any non-compliance with this policy by any other employee or contractor in terms of the provisions of the relevant agreement governing the relationship between us and them.

9.6. Exceptions and deviations

We may decide to relax or waive any aspect of this policy on a case-by-case basis in our sole discretion, but are under no obligation to do so. If we decide to do so, we must specifically authorise the exception or deviation.

9.7. Restrictions

We may restrict your access to IT at work if we do not believe that you are complying with this policy.

9.8. Liability and indemnity

You indemnify us against any claims arising out of a breach of this policy. We will not accept any liability for your use of IT when used for personal use, and you indemnify us against any liability. You need to clearly understand that your use of IT may cause us to be held legally liable.

9.9. Acceptance of terms

By accepting this policy, you are deemed to have read, understood, accepted, and agreed to be bound by all its terms.

9.10. Changes

We may change this policy at any time and where this affects your rights and obligations, we will notify you of any changes by email.

9.11. Reference documents

You must read this policy in conjunction with all applicable standards and procedures.

9.12. Enquiries

If you have any questions or concerns arising from this policy, please contact us.