Effective: 1 November 2016

Investec's IT acceptable usage policy

Information is a key asset of Investec and it must be appropriately managed and protected at all times. Information security is the responsibility of all employees and this policy sets out your obligations to safeguard Investec's competitive advantage and business continuity as well as ensuring the ongoing confidentiality, integrity and availability of our computer resources. For the purpose of this policy, "employees" include all persons who are contractually involved (either permanently or temporarily) with Investec in a managerial, employee or consultant capacity.

As an employee, you are responsible for protecting the information resources to which you have access. These resources include both electronic and physical information as well as the IT systems and devices which you use or possess. Investec resources are provided for day-to-day business requirements and limited, reasonable personal use:

- You are expected to use IT resources for legitimate business purposes and in a manner consistent with our policies and practices.
- The reasonable personal use of company IT resources is permitted. Excessive use will be regarded as an abuse of this privilege and dealt with accordingly.
- IT activity and communications on any system owned by Investec or connecting in any way to the Investec infrastructure may be monitored to protect the business and ensure compliance with our policies and procedures. Investec reserves the right to employ any tool / activity for monitoring, auditing and where necessary, controlling users' access to our networks and information systems. This includes email messages and Internet use.
- Failure to comply with the policies and practices of Investec may lead to disciplinary action and/or criminal prosecution.

Internet and email usage

When using Investec systems or connecting to our network for internet or email, the following is prohibited:

- Downloading or distributing copyright materials (including *inter alia* articles, music, movies and software). This excludes legal articles which are circulated by legal advisers and law firms and which, by their nature are copyrighted.
- Accessing or disseminating offensive, defamatory or discriminatory statements or material (including *inter alia* statements or material based on race, nationality, gender, sexual orientation, age, disability, religious or political beliefs).
- Accessing or distributing any obscene, pornographic, or otherwise distasteful content.
- Using unapproved peer-to-peer file sharing software.
- Seeking business opportunities, soliciting money for personal gain or searching for jobs outside Investec.
- Conducting or soliciting support for political, personal or religious causes.
- Knowingly or wilfully propagating malware.
- Sending unsolicited commercial email ("spam").
- Using private email accounts to conduct Investec business.
- Engaging in unlawful activity or any other activity likely to bring Investec into disrepute.

Social media

Social media encourages you to share information, to connect with people and to build relationships. It is your decision whether or not you participate in any digital network (e.g. Facebook, Twitter etc.) or any online publishing / discussion / chat rooms but be aware that anything posted or shared in social media or any digital channel can go viral and become public, no matter what your privacy settings may be. You are reminded that through your relationship with Investec, you have access to confidential information that cannot be made public.

Social media activity that contravenes this policy or negatively affects your performance, the performance of other employees, the reputation of Investec, its employees, clients, suppliers or business interests (collectively referred to as "Investec stakeholders") will be viewed in a serious light and where appropriate, disciplinary action will be taken.

- Legitimate activities may be conducted for certain job functions through social media.
- You are personally responsible for any content that you publish on any social media site or platform.
- Do not engage in activities on social media which may bring Investec into disrepute.
- Do not use social media in any way to attack or abuse Investec or its stakeholders.
- Do not post derogatory or offensive comments on social media. As an employee of Investec, you are required to conduct yourself in a manner that is aligned to our values.
- Do not publish photographs showing people's faces without their permission.
- Do not post non-public or confidential information about Investec or its stakeholders without the specific authorisation to do so (and this includes *inter alia* details of its IT infrastructure, policies or products).
- Do not comment on work-related legal matters unless you are an official spokesperson and have the required approval from Investec.
- Always respect copyright and fair-usage laws. You need to obtain permission before publishing the work of another party, and always refer to the source.
- If contacted about Investec on social media, do not respond without permission and guidance from Investor Relations or the head of Group Marketing.
- Do not use the Investec brand or logo without express approval from Investec Group Marketing.

Physical security

This is the first layer of defence in protecting Investec information against theft or unauthorised access:

- Access cards must be kept in your possession at all times. Report the loss or theft of your access card to Facilities immediately.
- Report any unusual activity or suspicious individuals to your line manager or Facilities.
- Meet visitors at the Investec main reception and do not have them sent to your area or allow them to walk around the building without an escort.

IT account and password security

You are required to safeguard your passwords (to access computers and information systems) against compromise and to report any suspected misuse:

- Do not share your password with anyone except for provision of IT technical support. If disclosed for this purpose, change it as soon as possible afterwards.
- Do not write your passwords down, they must be kept only in approved password management systems.
- Change your passwords at regular intervals, or as prompted, in line with Investec security standards.

- When changing your password, do not reuse any recent password or a derivation thereof.
- If your password has been accidentally disclosed or guessed by another person, change it immediately.
- It is strictly prohibited to use another employee's credentials to access Investec networks or systems.

Although different systems may have different password requirements, it is important to choose secure passwords:

- Use eight or more characters. Mix upper and lower-case letters, numbers and special characters.
- Do not create passwords using your names or personal data (e.g. date of birth, license plate). Avoid common words found in a dictionary and the word 'Investec'.
- Do not use the same passwords that you use for external and personal accounts or websites.

Computer security

The security of our information relies on the protection of our networks and systems. You are required to take steps to protect our systems against compromise:

- Never try to circumvent security mechanisms that protect against viruses and other forms of malware.
- Do not tamper with or disable any software installed on your system.
- Always lock your computer when you are away from your desk (use 'Windows' and 'L' keys).
- Secure your laptop with a cable lock, or store it in a locked cabinet or drawer.
- Do not connect unauthorised or non-Investec systems or devices to our network without the required approval and/or IT security checks.
- Any computer which is donated, sold or disposed of must be security wiped by Investec IT prior to its removal from our premises.

Mobile device security

You are required to exercise special care with mobile phones, tablets and portable storage devices as these are particularly vulnerable to loss, theft or compromise:

- Do not leave your mobile device unattended or unlocked.
- Securely lock away mobile devices when you are away from your desk and overnight.
- Mobile phones and tablets must have a pin code or password in line with Investec security standards.
- Notify the IT service desk and your line manager immediately if your mobile device is lost or stolen. If there is confidential data on a device that is lost or stolen, notify Compliance immediately
- If you are disposing of or reusing portable storage devices, these must be securely wiped by the IT service desk beforehand.

Cyber security

Criminals target both Investec's and your personal information. In order to protect yourself and the organisation, the following precautions must be taken:

- Do not click on links in email messages from unknown sources.
- Do not open unexpected or suspicious attachments, even if the sender is someone you know.
- Be suspicious of any email message with an urgent request for personal or financial information.

- Do not provide your Investec usernames or passwords on any website.
- Do not sign up for personal websites or online services using your Investec email address.
- Delete suspicious emails and report them to the IT service desk and risk manager.
- Internet browsing and downloading should be done with extreme caution.

Security incidents

Employees are required to be vigilant and to escalate any suspicious activity or security incident immediately:

- Any information breaches must be escalated to the relevant compliance officer or data protection officer.
- Report actual or suspected security incidents to the IT service desk and your risk manager.
- Do not engage or disclose any information about security incidents or breaches to external parties.
- Any security flaws or weaknesses that you discover must be reported to the relevant risk manager.
- If you think your system is infected or otherwise compromised, do not turn off your computer or answer any prompts; lock the system and notify the IT service desk and your risk manager immediately.

Working remotely

Working remotely increases the risk to Investec information. Appropriate steps must be taken to safeguard Investec information when out of the office:

- Always use the secure Investec remote access procedures provided by IT.
- Do not use your personal email accounts to send work related emails.
- Do not forward work emails or other Investec information to personal email addresses.
- Do not discard Investec documents in your home rubbish. Return these to the office for secure disposal.
- Ensure your home network has a strong password for wireless access.
- If flying, always carry your laptop and documents as hand luggage and keep them with you at all times.
- If leaving a laptop or documentation in a vehicle, always lock these in the boot.
- If you are staying in a hotel, lock laptops and work documents in a safe when you leave the room.
- Do not use public computers to access, store, or work on Investec information.
- You may only remove confidential documents from Investec's premises if authorised to do so.

Protecting confidential information

Information needs to be protected in line with its classification and business value:

- Ensure you know which information in your area is confidential or sensitive.
- Make the confidential nature of documents known to recipients by marking them appropriately.
- Do not store confidential information in openly accessible or public shared folders.
- Store critical files on your assigned network drives, where they are automatically backed up.

Physical information

Physical and paper-based information must be adequately protected and must not be left unattended:

- Use secure bins and shredders for destroying documents.
- Do not leave documents on printers, photocopiers or fax machines.
- Securely lock away sensitive documents. Do not leave them on your desk.
- Avoid discussing Investec information in public or in places where you could be overheard.
- Do not share or disclose Investec information with external parties unless authorised to do so.