General IT Policy

Pieter Smith

SECURITY
EXCELLENCE

Bidvest
PROTEA COIN

Contents

1 Introduction

The IT department oversees the maintenance and installation of network and communication systems as well as evaluate and approve hardware and software systems to enable automation of routine tasks, to facilitate communication and encourage collaboration to ensure optimal user productivity. It is important that authorized parties have timely and appropriate access to electronic information and communications systems, while safeguarding the information's confidentiality, security and integrity.

1.1 Document Location

This document is amended by the distribution of new revisions of all or part of the document to the named holders. The location of the latest and the older versions are

Revisions	**Location**	**Authorised**
Archived	IT – General\Policies\Policies and SoP\Archive	Pieter Smith
Current	IT – General\Policies\Policies and SoP	Pieter Smith

Copies of this document other than those listed above will not be revised; such copies are marked as UNCONTROLLED.

1.2 Scope

This document describes the general IT policies applicable to the organization, its employees and contractors. Other policies might take precedence over this policy in certain scenarios like data privacy and backup.

1.3 Accountability

It may be necessary for BPC IT staff to request the password of an individual employee during problem resolution. IT staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels. It is imperative for the user to not leave the support technician unattended during his/her investigation and to change his/her password the moment the issue has been resolved.

Failing to comply might result in disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

1.4 Access and disclosure

BPC reserves the right to access and disclose the content of a users' electronic and telephonic communications. This will however only be done for valid business reasons. Reasons may include but are not limited to:

- The need to solve technical problems.
- Investigation of theft or other crime.
- Prevention of unauthorised disclosure of confidential or personal information.
- Suspicion of abuse of systems and/or hardware.
- If required to do so by law.

2 Roles and responsibilities

IT is divided into 3 distinct sections:

2.1 Support Desk

The support desk ensures the speedy resolution of all first line requests and are the custodians of the ticketing system.

2.2 Advanced support

This section looks after the back office and ensure that all systems run optimally. This is the team that ensure the availability of the general infrastructure.

2.3 DevOps

The DevOps team maintains in-house developed systems and from time to time add new systems to the line-up.

2.4 Accounts and privileges

2.4.1 Application for a new account

All new employees need to be registered on the BPC domain. A domain account by default provides an email address and cloud storage via OneDrive for Business. The mailbox as well as the cloud storage is backed up to a 3rd party solution and the data is retained indefinitely.

The employees' line manager is responsible to complete the Domain User Form. The line manager and employee must sign the document.

It is important to note that:

1. HR and Payroll register the new employee within two months of employment. If no registration is found, the associated domain account will be placed in a disabled state.
2. Incorrectly completed documentation will result in the inability to match information to Payroll and the associated domain account will be disabled.
3. If the domain account is dormant for more than 3 months, it will be disabled and archived.

2.4.2 Suspicious Accounts

If an account is found to have been used in any illegal actions, it is disabled and investigated.

2.4.3 Anonymous Accounts

Anonymous accounts are allowed on a per case basis. These accounts are typically used for shift workers and registered under the managers name who takes responsibility for these accounts.

2.4.4 Service Accounts

Service Account are for internal IT use but treated in the same way as anonymous accounts. These accounts typically have elevated access, and more focus is placed on its security.

2.4.5 Support Accounts

Support Account are used by support consultants to assist with various tasks relating to outsourced services. These accounts are allocated to a responsible employee. These accounts remain in an expired state and the date is only moved upon request from the responsible employee.

2.4.6 Termination of contract

Monthly monitoring of terminated employee contracts are done. The removal process will commence in three stages:

Stage 1
- Set auto response message on email.
- Initiates log out on all devices
- Remove associated licenses

Stage 2 is a 30-day cooling off period.

Stage 3 Archive the domain account.
In this step the account is physically removed from the AD and no longer recoverable. Any data associated with the account that need to be recovered after archiving will have to be done via backup systems. Data is retained in the backup systems according to the backup policy.

2.4.6.1 Auto response message

```
Hi there,
Thank you for your email.
Unfortunately, this employee left Bidvest Protea Coin. If this is urgent, please contact Head Office
personnel at info@proteacoin.co.za or 012 665 8000.
Regards,
Bidvest Protea Coin
```

2.5 Internet usage

With the adoption of cloud services all employees will by default be granted access to internet services. This access is strictly for business purposes and is monitored on a continuous basis. A lot of effort is put in to make browsing safe and secure for everyone, but it is still up to each employee to practise safe browsing habits and to avoid clicking on suspicious links.

Internet access can be suspended if abused or any other reason that necessitate such action.

2.6 Electronic Mail

As a productivity enhancement tool, BPC encourages the business use of electronic communications.

Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. E-mail communication should follow the same standards expected in written business communications and public meetings.

2.6.1 Ownership

Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are the property of BPC.

2.6.2 Monitoring

BPC has the right to assess access, monitor, disclose or assist in intercepting and retrieve any communication for legitimate business reasons, including without limitation, compliance or non-compliance with this policy. Communication is monitored on a continuous basis.

2.6.3 E-mail use

The following use of the e-mail system is strictly prohibited:

The creation and exchange of messages that is offensive, harassing, obscene, pornographic, threatening, inciting violence, and propaganda for war or advocating hatred based on race, ethnicity, gender or religion. Contravening listed acts could lead to immediate dismissal.

- The exchange of proprietary information, trade secrets or any other privileged, confidential or company sensitive information. Confidential messages should include a warning regarding accidental transmission to an unintended third party.
- The creation and exchange of advertisements, solicitations, chain letters and other unsolicited e-mail as well as using the company's electronic communications systems for charitable endeavours, private business activities, or amusement/entertainment purposes are forbidden.
- The creation and exchange of information in violation of any copyright laws, for example music files.
- Altering or copying a message or attachment belonging to another user without the permission of the originator.
- Compromising the privacy of any password and/or publishing any password to another party.
- Addressing messages to everyone you know rather than recipients who need to know.
- Messages must be constructed professionally (spelling, grammar) and efficiently (subject filed, attachments).
- Incidental personal use is permissible so long as:
    - It does not consume more than a trivial amount of resources
    - It does not interfere with staff productivity
    - It does not pre-empt any business activity

2.7 Web-based information

- Users of the intranet shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system.
- Access to web pages should be controlled according to the level of confidentiality of the information and the risk involving access thereto. The implementation of these access control mechanisms should regularly be checked for possible security flaws and questionable risks.
- Intranet information will be securely extended to all employees by providing a controlled and secured centralised point of access to all web-based information. External customers, i.e., suppliers and trading partners will only be allowed access to the intranet once a valid business need has been identified and an NDA has been signed.

2.8 VPN and remote access to information resources

- The remote connection facility provided by BPC will only be used for official purposes.
- Authorized employees, contractors and other authorized parties will be the only persons permitted to use the remote connection facility to access information resources, with proper safeguards.
- Should you be issued with a 3G card it will be for official company use only. There is a monthly data limit on all 3G accounts and should not be exceeded, should it be found that the device was misused, the company might recover these costs from you.

2.9 Password Implementation

a) Passwords should consist of a minimum of 8 characters. Words which can be deduced from information about you, do not constitute a secure password.
b) Passwords must contain an uppercase character, at least 1 special character and three non-reoccurring digits.
c) MFA is enabled on all accounts be default. Exceptions will only be considered in cases where it is not practical like service accounts and all cases are to be approved by the Group IT manager. Changing of password regularly is still encouraged.

d) Passwords may never be written down.
e) All passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties. Contact IT in such an event.
f) You are responsible for the security of your username and password and will be held liable for any misuse of resources where your username and password has been used. It is therefore imperative that you protect your password.
g) Disciplinary action will be taken against employees sharing their usernames and passwords

2.10 Hardware

Devices are owned by the department who procured it or to who it has been transferred over its life. The devices should be kept for the replacement employee should the original user resign. If the position is declared obsolete the equipment is returned to IT for re-distribution.

In the event of equipment being damaged or not functioning any longer, repairs are requested via the IT helpdesk (helpdesk@proteacoin.co.za) if during the helpdesk's investigation it is determined that the equipment was damaged due to negligence, the costs may be recovered from the user. The same goes for lost or stolen equipment. Ultimately the cost centre manager will be the decision maker on whether costs will be recovered.

2.11 Compliance training

Compliance training is required on Data Privacy and other policies from time to time and is compulsory for all employees of BPC. Training must be available for permanent employees as well as contractors, consultants and temporary employees. Any changes to policies must be communicated to all employees of BPC.

2.12 Processing of personal information

Personal information may only be processed in accordance with the official Data Privacy Policy.

2.13 Governance

2.14 Ownership of this policy

Ownership of this policy is vested with the **Group IT Manager**.

2.15 Approval

This policy must be approved by the **Group IT Manager**.

2.16 Non- Compliance

Non-compliance with this policy, standards, procedures, or the like, is a disciplinary offense and may result in disciplinary action and possible dismissal.

2.17 Implementation

The executive of each business area is accountable for the implementation and adherence to this policy in his/her respective business areas.

2.18 Disciplinary Action

Where a complaint or an infringement investigation has been finalised, BPC may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, BPC will undertake to provide further awareness training to the employee.

Any gross negligent or the wilful mismanagement of personal information will be considered a serious form of misconduct for which BPC may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence. Examples of immediate actions that may be taken after an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets to limit any prejudice or damages caused.

2.19 Indemnity

BPC has no responsibility, whether by law or otherwise, because of the employee utilizing email or internet access facilities provided by BPC (as above) for personal use. The employee irrevocably and unconditionally indemnifies BPC against any loss, costs, damages or other claims which BPC or the employee may suffer/incur as a result of the employee utilizing email and internet access facilities provided by BPC (which email, and internet access facilities are provided by BPC solely for business purposes) for personal use.

2.20 Review

This policy must be reviewed on an annual basis or more frequently if deemed necessary.

2.21 Glossary

AD	Active Directory
BPC	Bidvest Protea Coin and all its subsidiaries and business areas.
MFA	Multi-Factor Authentication.