INFORMATION SECURITY POLICY

ISO 27001 DOCUMENT

- *Contents*

1 Introduction

As a modern, forward-looking business, Fincra recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation and to suit the purpose of its organisation, Fincra has implemented an Information Security Management System (ISMS) in line with the International Standard for Information Security, ISO/IEC 27001.

The impact of an information security incident will obviously depend upon its nature and a comprehensive risk assessment is maintained to assess and mitigate those that can be reasonably identified.

In general terms the potential impact of an incident or breach will be shown in one or more of the following key business areas:

- Loss of sales revenue
- Risk to life on health and safety grounds
- Loss of reputation or customer confidence
- Inability to meet our legal obligations
- Breach of contractual obligations
- Loss of business opportunity

This information security policy forms a key part of our set of controls to ensure that our information is protected effectively and that we can meet our obligations to our customers, shareholders, employees and partners. Hence Fincra is committed to satisfy all applicable requirements to ensure the confidentiality, integrity and availability of its information asset and ensure continuous improvement of the ISMS.

Non-compliance with this policy could have a significant effect on the efficient operation of Fincra and may result in financial loss and an inability to provide necessary services to our customers.

If any employee is found to breach this policy, the following disciplinary action would be taken depending on the severity of the breach, this may include:

- An informal warning from a manager
- A formal verbal or written warning for misconduct
- Dismissal for gross misconduct
- Criminal proceedings

- Civil proceedings to recover damages

If you do not understand the implications of this policy or how it may apply to you, seek advice in the first instance from your immediate manager.

This policy would be reviewed yearly and upon any significant change to ensure continuity, suitability, adequacy and effectiveness.

This policy is a public document and must be communicated to all within the organization and stored on the Google drive for easy access. It would also be made available to all interested parties where appropriate.

This policy would satisfy any applicable requirements related to information security and would also ensure the continuous improvement of the ISMS.

Scope

This policy supports the security policy and applies to all activities of Fincra included in the scope of the Information Security Management System.

1.1.1 Objectives

- Ensure the continuity of critical business processes
- Ensure effective management and efficient Information Security Management
- Provide a choice of appropriate and proportionate security controls to protect the assets and thus give confidence to interested parties
- Ensure that all Information processed, stored and traded by the organisation is of absolute integrity.

1.1.2 Principles

- This policy has been approved by management and is subject to an annual review
- Fincra should take into account all legal, regulatory and contractual requirements in the management of the information security management system in order to avoid breaching its legal statutory, regulatory and contractual obligations and security requirements.
- The legal and regulatory requirements will be met in priority, even if they are inconsistent with the policy described here.

- Fincra shall establish, implement, operate, monitor, review, maintain and improve an ISMS based on a documented approach to risk activity and compliance with all requirements of ISO 27001.

2 EMAIL POLICY

2.1 Introduction

Email has now become a vital business tool for communicating both internally and with customers and suppliers. However, because of its flexibility and general availability, the use of email carries with it a number of significant risks and all users must remain vigilant and adopt good practice when sending and receiving emails to ensure that the information involved in electronic messaging is adequately protected.

This policy document tells you how you may use Fincra's email facility, including what you must and must not do. It applies to all use of the facility whatever the means or location of access e.g. via mobile devices or outside of the office.

The email facility is provided to you to help carry out the business of the organization. However you may use email for some personal purposes within the constraints set out in this policy.

If you do not understand the implications of this policy or how it may apply to you, you should approach your line manager in the first instance.

2.2 Sending and Receiving Email

Fincra-provided email address must always be used when communicating with others on official business. You should not use a personal email address for this purpose. Guidelines on the sending of classified information (information classified as Protected / internal, Restricted or Confidential) via email must be observed at all times. These are set out in document Fincra Information Security Classification Guidelines.

All emails sent from Fincra's email address remain the property of Fincra and are considered to be part of the corporate record. All Fincra's emails should be considered to be official communications from Fincra and treated accordingly.

Fincra maintains its legal right to monitor and audit the use of email by authorised users to assess compliance to this policy. This will be done in accordance with the provisions of relevant legislation.

Deletion of an e-mail from an individual account does not necessarily mean that it has been permanently removed from Fincra's IT systems and such emails may still, be subject to audit and review.

All e-mails sent from Fincra's addresses to recipients outside of the Fincra will automatically carry the following disclaimer:

"The information contained in this message is intended for the addressee only and may contain classified information. If you are not the addressee, please delete this message and notify the sender; you should not copy or distribute this message or disclose its contents to anyone. Any views or opinions expressed in this message are those of the individual(s) and not necessarily of Fincra. No reliance may be placed on this message without written confirmation from an authorised representative of its contents. No guarantee is implied that this message or any attachment is virus free or has not been intercepted and amended."

Users should remain aware that it cannot be guaranteed that an email will be received or read by a recipient and that messages can be interpreted in different ways according to the culture, role and even prevailing mood of the individual reading it. You should therefore at all times consider whether the use of email is an appropriate means of conveying the information involved and whether an alternative such as the telephone would be preferable, particularly if the message is urgent or complex.

Particular care must be taken when addressing emails that include classified information to prevent accidental transmission to unauthorised recipients. Beware of the auto-completion feature of some email clients where the system suggests recipients based on the characters typed in so far.

Do not use auto-forwarding e.g. whilst on holiday, if there is a possibility that this may result in classified information being forwarded to a recipient that does not have sufficient security clearance for the level of information involved.

Users should avoid sending unnecessary messages to distribution lists, particularly those with wide circulation such as the "global list" of all employees. Where required, such emails should be sent via Fincra's communications department.

Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.
Sending mail outside the Fincra Group network requires the approval of the Information Security Manager.

Emails from a Fincra email address should be considered in the same way as other more formal methods of communication. Nothing should be sent externally which might affect Fincra's reputation or affect its relationships with suppliers, customers or other stakeholders.

In particular, users should not send emails containing material which is defamatory, obscene, does not comply with Fincra's Equality and Diversity Policy or which a recipient might otherwise reasonably consider inappropriate. If you are not sure whether your intended message falls into this category, please consult your line manager before sending the email.

Fincra's Official email addresses and facilities should not be used:

- for the distribution of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations
- to send material that infringes the copyright or intellectual property rights of another person or organisation
- for activities that corrupt or destroy other users' data or otherwise disrupt the work of other users
- to distribute any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
- to send anything which is designed or likely to cause annoyance, inconvenience or needless anxiety to others
- to convey abusive, threatening or bullying messages to others
- to transmit material that either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs. Anyone with the intent of using Fincra's email to transmit discriminating materials on the grounds of race, gender etc has comitted an offence according to the Cybercrime Act 2015 section 26.
- for the transmission of defamatory material or false claims of a deceptive nature
- for activities that violate the privacy of other users
- to send anonymous messages - i.e. without clear identification of the sender
- for any other activities which bring, or may bring, Fincra into disrepute

If you receive unsolicited junk email or spam, it is advised that you delete such messages without reading them. Do not reply to the email as this can confirm the existence of a valid address to the sender, resulting in further unwanted communications.

2.3 *Maintaining your email account*

Your mailbox will be set up with a limitation on its size. This is in order to prevent the available storage capacity from being exceeded and to ensure the cost-effective use of email.

You should manage your email account(s) to remain within the mailbox size limit, making use of the archiving facility included in most email clients where possible. If your mailbox has filled up, contact the Information Security for advice in the first instance.

Where possible, make use of links to files within email messages rather than attaching a copy of the file, particularly if the email message has a wide distribution. This will prevent other user's mailboxes from filling up and so avoid consequent disruption.

Computer viruses, adware and other malware are small programs that can have a negative effect on your computer and your use of the internet and can expose the Fincra's information to extreme risk. Such viruses can be inadvertently downloaded and installed via emails received into your inbox. The organisation provides anti-virus software which runs on every computer that has access to the network and should detect any viruses before they have been installed.

If you believe you may have a virus or you have been sent an email that may contain one, please report this to the Information Security Unit immediately. Do not open any attachments you believe may contain a virus.

In addition, you must not:

- transmit by email any file attachments which you know to be infected with a virus
- download data or programs of any nature from unknown sources
- disable or reconfigure the installed anti-virus system operating on a computer used to access email facilities
- forward virus warnings other than to the Information Security

IT Security will ensure that all emails are virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is deliberately or accidentally sent to another organisation, Fincra could be held liable if the transmission could be considered negligent.

2.4 Email Monitoring

Email usage within the organisation system is monitored and recorded centrally in order to:

- plan and manage its resource capacity effectively
- assess compliance with policies and procedures
- ensure that standards are maintained
- prevent and detect crime
- investigate unauthorised use

Monitoring will be undertaken by staff specifically authorised for that purpose. Consistent monitoring procedures will be applied to all users and may include checking the contents of email messages.

In the event that a manager suspects that the email facilities are being abused by a user, they should contact the Information Security Manager. All such reports will be investigated according to documented procedures and where appropriate, evidence provided. There is also a requirement to provide such information to regulatory or legislative bodies in accordance with the law.

Users must not access another user's email account unless they have obtained permission from the owner of the account or their line manager. In such cases this should be for legitimate business reasons and only emails which may reasonably be judged to be relevant to the question in hand should be opened.

3 Using the Internet

This policy document tells you how you may use the Fincra Internet facility. It outlines your personal responsibilities and informs what you must and must not do.

The objective of this Policy is to direct all users of the internet facility by:

- Providing guidance on expected working practice
- Highlighting issues affecting use
- Describing the standards that users must maintain
- Stating the actions that may be taken to monitor the effectiveness of this policy

- Warning users about the consequences of inappropriate use of the internet service

The Internet facility is made available for the business purposes of the organisation. A certain amount of personal use is permitted in accordance with the statements contained within this policy.

It is recognised that it is impossible to define precise rules covering all Internet activities available and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

This policy covers all internet facilities that are provided by Fincra for the purpose of conducting and supporting official business activity through the organisation's network infrastructure and all portable computer devices.

This policy is intended for all board members, committees, departments, partners, employees, contractual third parties and agents of the organisation who have been designated as authorised users of internet facilities.

This Internet Acceptable Usage Policy should be applied at all times whenever using the provided Internet facility. This includes access via any device including a desktop computer or a smartphone.

This policy aims to mitigate the following risks:

- Loss of reputation due to inappropriate use of internet facilities by staff
- Lack of compliance against legal or regulatory requirements
- Malicious electronic attacks using the Internet as a route in to the network

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers. If any user is found to have breached this policy, they will be subject to disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice in the first instance from your immediate manager.

3.1 Business Use of the Internet Service

Your Internet account should be used in accordance with this policy to access anything in pursuance of your work including:

- Access to information that is pertinent to fulfilling the organization's business obligations
- The capability to post updates to organisation-owned and/or maintained web sites
- An electronic commerce facility (e.g. purchasing equipment for the organisation)
- Research

Information obtained from internet sources must be confirmed before use for business purposes.

3.2 Personal Use of the Internet Service

The organisation permits personal use of the Internet in your own time (for example during your lunch-break), provided it does not interfere with your work. Any exception to this is at the discretion of your line manager.

The organisation is not, however, responsible for any personal transactions you enter into - for example in respect of the quality, delivery or loss of items ordered. You must accept responsibility for, and keep the organization protected against, any claims, damages, losses or the like which might arise from your transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via the Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the organisation.

You should ensure that personal goods and services purchased are delivered to your home or other personal address and not delivered to organisation property.

If you are in any doubt about how you may make personal use of the Internet Service you are advised not to do so.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of the organisation and may be accessed at any time by the organization to ensure compliance with all its statutory, regulatory and internal policy requirements.

3.3 Internet Account Management, Security and Monitoring

The organisation will provide a secure logon-id and password facility for your Internet account. The Information Security Unit is responsible for the technical management of this account.

You are responsible for the security provided by your Internet account user name and password. Only you should know your user name and password and you should be the only person who uses your Internet account.

You should not use anyone else's user name to access the Internet.

The provision of Internet access is owned by the organisation and all access is recorded, logged and interrogated for the purposes of:

- Monitoring total usage to ensure business use is not impacted by lack of capacity
- The filtering system monitors and records all access for reports that are produced for line managers and auditors

3.4 Prohibited Uses of the Internet Service

Except where it is strictly and necessarily required for your work, for example IT audit activity or other investigation, you must not use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive. Anyone who uses a computer or network for viewing or producing child pornography and other illegal material has commited a crime in accord with section 23, 24 and 26 of the Cysbercrime Act 2015.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs
- Subscribe to, enter or use online gaming or betting sites
- Subscribe to or enter "money making" sites or enter or use "money making" programs.

- Run a private business
- Download any software that does not comply with the organisation's Software Policy.
- No insecure ports, protocols or services are to be used on the internet by any user.

The above list gives examples of "unsuitable" usage but is neither exclusive nor exhaustive. "Unsuitable" material would include data, images, audio files or video files the transmission of which is illegal and material that is against the rule, essence and spirit of this and other organisational policies.

The organisation will take steps to block the following categories of websites:

- Illegal.
- Pornographic.
- Violence.
- Hate and discrimination.
- Offensive.
- Weapons.
- Hacking.
- Web chat.
- Gambling.
- Dating.
- Radio stations.
- Games.
- Streaming Media.

If you have inadvertently attempted to access such as site you should inform the Information Security Unit immediately.
Violation of these usage policies is grounds for being reprimanded, suspended or terminated.

4 Password policy

The creation of strong passwords, their protection and frequency is of paramount importance to Fincra as such this policy covers all personnel who have or are responsible for any account that requires a password on any system that resides on any Fincra domain, has access to the Fincra network, or stores any confidential information of the Organisation.

Passwords should not contain the user's name or relative's name, employee number, birthday, telephone number, address, or any other information about the user that could be easily guessed or discovered.

Users should ensure that passwords do not contain common words or words found in any dictionary. If the password has been given to someone else, then it must be changed immediately.

Passwords must have at least 8 characters or more and must contain a mixture of alpha and numeric characters, as well as special characters. The password cannot contain the user's login name. An example of a strong password is LeaddwAke916@&

To prevent accidental disclosure the following precautions must be taken:

Passwords must not be disclosed to anyone, including anyone claiming to be user support staff or vendor support staff. Anyone who discloses his or her passwords either knowingly or intentionally for an unlawful gain or purpose has committed a crime and is liable to not more than 2 years imprisonment or a fine of 5million naira or to both fine and imprisonment in line with the Cybercrime Act 2015, section 28 (3).

Users should not communicate his/her password or password paraphrase in an email.
Passwords should not be written down.
New passwords cannot be a simple change of the previous password, e.g. adding a number at the beginning or end, changing one letter or number.
The Principle of Least Privilege must be used in assigning privileges to accounts.
System configuration settings are set to require that system/session idle timeout features have been set to a period of five (5) minutes or less
Passwords cannot be reused until after three (3) passwords.
Passwords must be changed as soon as possible after a compromise and within one business day.
User can change his/her password anytime with the system.
User accounts will be locked after 3 consecutive unsuccessful login attempts.
System configuration settings will be set to release locked accounts after a period of five (5) minutes or less.
System configuration settings can be set for service accounts not to be locked or not to have their passwords changed; however, compensating controls must be in place to regularly review the use and misuse of service accounts or authentication failures.

5 Access Control

The control of access to our information assets is a fundamental part of a defence in depth strategy to information security. If we are to effectively protect the confidentiality, integrity

and availability of classified data then we must ensure that a comprehensive mix of physical and logical controls is in place.

But our policy with regard to access control must ensure that the measures we implement are appropriate to the business requirement for protection and are not unnecessarily strict. The policy therefore must be based upon a clear understanding of the business requirements as specified by the owners of the assets involved.

These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service
- Relevant legislation that may apply e.g. the Cybercrime Act 2015
- The regulatory framework in which the organization and the system operates
- Contractual obligations to external third parties
- The threats, vulnerabilities and risks involved
- The organization's appetite for risk

Business requirements should be established as part of the requirements-gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

In addition to the specific requirements, a number of general principles will be used when designing access controls for Fincra systems and services. These are:

- Defence in Depth – security should not depend upon any single control but be the sum of a number of complementary controls
- Least Privilege – the default approach taken should be to assume that access is not required, rather than to assume that it is
- Need to Know – access is only granted to the information required to perform a role, and no more
- Need to Use – Users will only be able to access physical and logical facilities required for their role

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that occur.

Anyone who without authorization, intentionally accesses a computer or network in whole or part for fraudulent practices or to obtain data against the approval of Fincra has commited

an offence and is liable to 5years imprisonment or a fine of 5million naira or to both fine and imprisonment. This is in accordance with the Cybercrime Act 2015, section 6.

5.1 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

5.2 User Registration and Deregistration

A request for access to the organisation's network and computer systems must first be submitted to the Information Security Unit for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are carried out and correct authorisation is obtained prior to user account creation. The principle of segregation of duties will apply so that the creation of the user account and the assignment of permissions are performed by different people.

Each user account will have a unique user name that is not shared with any other user and is associated with a specific individual i.e. not a role or job title. Generic user accounts i.e. single accounts to be used by a group of people should not be created as they provide insufficient allocation of responsibility.

An initial strong password should be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When an employee leaves the organisation under normal circumstances, their access to computer systems and data must be suspended at the close of business on the employee's

last working day. It is the responsibility of the line manager to request the suspension of the access rights to Information Security.

In exceptional circumstances where there is perceived to be a risk that the employee may take action that may harm the organisation prior to or upon termination, a request to remove access may be approved and actioned in advance of notice of termination being given. This precaution should especially apply in the case where the individual concerned has privileged access rights e.g. domain admin.

User accounts should be initially suspended or disabled only and not deleted. User account names should not be reused as this may cause confusion in the event of a later investigation.

5.3 User Access Provisioning

Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general this should be role-based i.e. a user account will be added to a group that has been created with the access permissions required by that job role.

Group roles should be maintained in line with business requirements and any changes to them should be formally authorised and controlled via the change management process.

Ad-hoc additional permissions should not be granted to user accounts outside of the group role; if such permissions are required this should be addressed as a change and formally requested.

5.4 Removal or Adjustment of Access Rights

Where an adjustment of access rights or permissions is required e.g. due to an individual changing role, this should be carried out as part of the role change. It should be ensured that access rights no longer required as part of the new role are removed from the user account. In the event that a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role should be requested via change management. Due consideration of any issues of segregation of duties should be given.

Under no circumstances should administrators be permitted to change their own user accounts or permissions.

5.5 *Management of Privileged Access Rights*

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general, technical users (such as IT support staff) should not make day to day use of user accounts with privileged access, rather a separate "admin" user account should be created and used only when the additional privileges are required. These accounts should be specific to an individual e.g. "Tolulope Onijigin Admin"; generic admin accounts should not be used as they provide insufficient identification of the user.

Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

The use of user accounts with privileged access in automated routines such as batch or interface jobs should be avoided where possible. Where this is unavoidable the password used should be protected and changed on a regular basis.

5.6 *User Authentication for External Connections*

In line with the network security policy the use of modems on non-organization owned PCs or devices connected to the organisation's network can seriously compromise the security of the network. Specific approval must be obtained from Information Security before connecting any equipment to the organisation's network.

Where remote access to the network is required via VPN, a request must be made via Dashlane or to the Information Security Unit. A policy of using two factor authentication for remote access should be used in line with the principle of "something you have and something you know" in order to reduce the risk of unauthorised access from the Internet.

5.7 *Supplier Remote Access to the Organisation's Network*

Partner agencies or 3rd party suppliers must not be given details of how to access the organisation's network without permission from the Information Security Unit. Any changes to supplier's connections (e.g. on termination of a contract) must be immediately sent to the IT Service Desk so that access can be updated or ceased. All permissions and access methods must be controlled by Information Security.

Partners or 3rd party suppliers must contact Information Security on each occasion to request permission to connect to the network and a log of activity must be maintained. Remote access software and user accounts must be disabled when not in use.

5.8 Review of User Access Rights

On a regular basis (at least annually) asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This will be to identify:

- People who should not have access (e.g. leavers)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification e.g. generic or shared accounts
- Any other issues that do not comply with this policy

This review will be performed according to a formal procedure and any corrective actions identified and carried out.

A review of user accounts with privileged access will be carried out by the Information Security Manager on a quarterly basis to ensure that this policy is being complied with.

5.9 User Authentication and Password Policy

A strong password is an essential barrier against unauthorised access. Unfortunately this area is often proven to be the weak link in an organisation's security strategy and a variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and biometric techniques.

Fincra's policy is to make use of additional authentication methods based on a risk assessment which takes into account:

- The value of the assets protected
- The degree of threat believed to exist
- The cost of the additional authentication method(s)
- The ease of use and practicality of the proposed method(s)
- Any other relevant controls in place

Use of multi-factor authentication methods should be justified on the basis of the above factors and securely implemented and maintained where appropriate.

Whether single or multi-factor authentication is used, the quality of user passwords should be enforced in all networks and systems using the following parameters:

Parameter	Value
Minimum length	8
Maximum length	16
Re-use cycle	Cannot be the same as any of the previous 6 passwords
Characters Required	At least one alphabet (Lower and upper) At least one symbol At least one number
Password similarity	New password cannot share more than three characters in the same position as the old password
Change Frequency	At least every 30 days
Account lockout	On 3 incorrect logon attempts
Password prompt	7-10 days to expiration of password
Account lockout action	Account will automatically be re-enabled within 3-5 minutes
Other controls	Password cannot contain the user name

Any exceptions to these rules must be authorised by the Information Security Manager.

5.10 User Responsibilities

In order to exercise due care and try to ensure the security of its information, Fincra expends a significant amount of time and money in implementing effective controls to lessen risk and reduce vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems in their day to day roles. Many recent high profile security breaches have been largely caused by unauthorised access to user accounts resulting from passwords being stolen or guessed.

It is vital therefore that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organisation.

In order to maximise the security of our information every user must:

- Use a strong password i.e. one which is in line with the rules set out in this policy
- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or electronically e.g. in a file or email
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended connected to the network is locked or logged out
- Leave nothing on display that may contain access information such as login names and passwords
- Inform the IT Information Security Unit of any changes to their role and access requirements

Failure to comply with these requirements may result in the organisation taking disciplinary action against the individual(s) concerned.

5.11 System and Application Access Control

As part of the evaluation process for new or significantly changed systems, requirements for effective access control should be addressed and appropriate measures implemented.

These should consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts
- Definition of roles or groups to which user accounts can be assigned
- Allocation of permissions to objects (e.g. files, programs, menus) of different types (e.g. read, write, delete, execute) to subjects (user accounts and groups)
- Provision of varying views of menu options and data according to the user account and its permission levels
- User account administration, including ability to disable and delete accounts
- User logon controls such as
    - Non-display of password as it is entered

  - Account lockout once number of incorrect logon attempts exceeds a specified threshold
  - Provide information about number of unsuccessful login attempts and last successful logon once user has successfully logged on
  - Date and time-based logon restrictions
  - Device and location logon restrictions
- User inactivity timeout
- Password management, including
  - Ability for user to change password
  - Controls over acceptable passwords
  - Password expiry
  - Hashed/encrypted password storage and transmission
- Security auditing facilities, including logon/logoffs, unsuccessful logon attempts, object access and account administration activities

Where bespoke software development is undertaken, program source code should be protected from unauthorized access in accordance with Fincra Secure Development Environment Guidelines.

Access to utility programs that provide a method of bypassing system security (e.g. data manipulation tools) should be strictly controlled and their use restricted to identified individuals and specific circumstances e.g. as part of a named project or change.

6 Physical Access and Environmental Control

To prevent unauthorised physical access, damage and interference to the Fincra's information and information processing facilities, security perimeters should be defined and used to protect areas that contain sensitive or critical information and information processing facilities.

The date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorised purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means;

Security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

All employees, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

Employees should not tailgate or swipe their access cards for anyone else.

Perimeters of a building or site containing information processing facilities should be physically protected.

A manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorised personnel only;

Physical barriers should, where applicable, be built to prevent unauthorised physical access and environmental contamination;

All fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner;

Suitable intruder detection systems should be installed and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;

Information processing facilities managed by Fincra should be physically separated from those managed by external parties.

7 Systems Operation / Administration

It is a prerequisite that IT personnel effectively perform IT administrative and operational activities. To do so, the following guidelines should be followed:

IT personnel must have knowledge about a wide range of security risks and which need to be managed.

Closely monitor files written by the Fincra's system(s) containing details of the changes made to records, and to the operational environment.

Review error logs regularly from each production system.

Deletion of users who have been inactive on the Google Workspace for 180 days.

Decommissioning of workstations that have been inactive on the Sophos for 60 days and above.

8 Change Management

Changes to Fincra, business processes, information processing facilities and systems that affect information security should be controlled.

The Change Management process should include:

Scope of the change management process.

Responsibility and accountability for managing and coordinating change.

Cross-functional process mapping of the change process within the organisation and with other affected parties.

Methodologies for classification and prioritisation of changes.

Determination of change impact or risk

Handling of changes and change reversals

Planning and testing of changes

Verification that information security requirements have been met

An emergency change process to enable quick and controlled implementation of changes needed to resolve an incident

Performance of post-implementation review and analysis

Review and analysis of key performance indicators
Approval of proposed changes

Communication of change details to all relevant persons;

Fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Version control.

9 Business Continuity

Information security continuity would be embedded in Fincra's business continuity management systems.

Perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations. Exercise and test the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives.

Exercise and test the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives

Review the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

Business continuity plans should be tested at least twice a year.

10 Clear Desk and Clear Screen

Sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

Computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication

mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

Unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented;

Media containing sensitive or classified information should be removed from printers immediately

Secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

11 People Operations Security

To ensure that employees and contractors understand their responsibilities and are suit-able for the roles for which they are considered, the following measures should be taken prior to employment, during employment and termination / change of employment.

Background verification checks should be conducted and should contain the following:

Availability of satisfactory character references, e.g. one business and one personal;

Verification (for completeness and accuracy) of the applicant's curriculum vitae;

Confirmation of claimed academic and professional qualifications;

Independent identity verification (passport or similar document);

More detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, Fincra should make sure the candidate:

Has the necessary competence to perform the security role;

Can be trusted to take on the role, especially if the role is critical for Fincra

Employees and contractors must sign a non-disclosure agreement if access to confidential information is given.

Management require all employees and contractors to apply information security in accordance with its established policies and procedures.

All employees of Fincra and, where relevant, contractors must receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

There must be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

Information security responsibilities and duties that remain valid after termination or change of employment must be defined, communicated to the employee or contractor and enforced

12 Incident Management

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses, management responsibilities and procedures must be established.

Information security events must be reported through appropriate management channels as quickly as possible.

Employees and contractors using Fincra's information systems and services must be required to note and report any observed or suspected information security weaknesses in systems or services

Information security events must be assessed and it must be decided if they are to be classified as information security incidents.

Information security incidents must be responded to in accordance with the documented procedures

Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents

Procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence must be defined and applied.

The Incident Response Plan is to be tested annually

13 Removable Media

In Fincra, the use of removable media is not allowed however some personnel who require such for the official duties are granted the right to use removable media upon approval from their supervisor and may require the consent of the CISO where applicable. Where removable media of any format (CD, DVD, Memory stick, Tapes etc.) is used to store sensitive data an assessment must be made of whether an alternative, more secure method can be used and if not, how best to secure the current method so that the risk to Fincra is minimised.

Such existing uses may include:

Transfer of data to third parties e.g. suppliers, contractors, other agencies
Taking data home to work on
Backups of data in addition to scheduled server backups
Transfer data between devices e.g. PC to PDA

In the event that an existing use is not in the above list but contravenes the information security policy, an alternative method of achieving the desired end result still needs to be identified. See Fincra removable media assessment policy for more information

14 Acceptable Use

Inappropriate use of Fincra's computer equipment exposes the organization to risks including virus attacks, compromise of the organizations network and services as well as legal issues. This policy is therefore is outlined to protect staffs and the Organization as a whole.

All operating systems, applications and databases within the organisation are to be configured and used strictly for business operations only. They should also be appropriately hardened and secured in accordance with industry standards and for business requirements as needed.

Unless given prior consent by the appropriate personnel, operating systems, applications and databases may not be added, removed or modified.

Any operating system, applications and database obtained without proof of purchase and licensing rights will not be allowed onto the network.

All users (system administrative users) must be responsible for the proper use of these operating systems, applications and databases.

Any activity that may potentially compromise Fincra's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organisation because of misuse of these operating systems, applications and database will not be tolerated.

All applications (internally developed and commercially purchased) are to be configured and used strictly for business operations.

All applications are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. All users (coders/developers, end-users) must be responsible for the proper use of these applications.

All users and their respective functions for any applications and database system administrative rights and subsequent activities are subject to audit and reviews as needed.

All users (database administrators, end-users of databases, etc.) must be responsible for the proper use of these technologies.

All removable electronic media devices are to be configured and used strictly for business operations.
All removable electronic media devices are to be appropriately hardened and secured in accordance with industry standards and for business requirements as needed. All users must be responsible for the proper use of these technologies.

Users are prohibited from copying, moving or storage of cardholder data onto local hard drives and removable electronic media when accessing such data via remote access technologies

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages would not be entertained.

Unauthorised use, or forging, of email header information is also not entertained.

Use of unsolicited email originating from within Fincra's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Fincra or connected via Fincra's network.

Blogging by employees, whether using Fincra's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Fincra's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Fincra's policy, is not detrimental to Fincra's best interests, and does not interfere with an employee's regular work duties. Blogging from Fincra's systems is also subject to monitoring.

Fincra's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Fincra confidential or proprietary information, trade secrets or any other material covered by Fincra's Confidential Information policy when engaged in blogging.

Staffs shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Fincra and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Fincra's Non-Discrimination and Anti-Harassment policy.

Staffs may also not attribute personal statements, opinions or beliefs to Fincra when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Fincra. Employees assume any and all risk associated with blogging.

15 Mobile Computing

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful the number of tasks that can be achieved away from the office grows. However, as the capabilities increase so do the risks. Security controls that have evolved to protect the static desktop environment are easily bypassed when using a mobile device outside of the confines of an office building.

Mobile devices include items such as:

- Laptop and notebook computers
- Tablet devices
- Smartphones
- PDAs

The purpose of this policy is to set out the controls that must be in place when using mobile devices. It is intended to mitigate the following risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of classified information through observation by the public
- Introduction of viruses and malware to the network
- Loss of reputation

It is important that the controls set out in this policy are observed at all times in the use and transport of mobile devices.

15.1 General

- Only mobile devices provided by Fincra should be used to hold or process classified information on behalf of the organisation except expressly approved or authorised by Senior Management

- You should not use your own devices for business purposes except expressly approved or authorized by Senior Management.

- If you are required to make use of mobile equipment, you will be provided with an appropriate device(s) which will be configured to comply with the organisation's policies.

- Support will be provided by Information Security who may at times need access to your device for problem resolution and maintenance purposes.

15.2 Physical Protection

- You must ensure that the device is transported in a protective case when possible and is not exposed to situations in which it may become damaged.
- Do not leave the device unattended in public view, such as in the back of a car or in a meeting room or hotel lobby.
- Do not remove any identifying marks on the device, such as a company asset tag or serial number.
- Ensure that the device is locked away when being stored and that the key is not easily accessible.
- Faults with the device must be logged with Information Security.
- Do not add peripheral hardware to the device without the approval of the Information Security Unit.
- The Information Security Unit should be consulted before the device is taken out of the country. This is to ensure that it will work and to consider any insurance implications.

15.3 Cryptographic Techniques

- Where possible, the device will be secured so that all of the data on it is encrypted and so is only accessible if the password is known.
- If the device is supplied with encryption, do not disable it.

15.4 Backups

- Changes to files held on the device may not be backed up on a regular basis if it is not connected to the corporate network for a period of time. Try to schedule some time in to achieve this on a regular basis.
- Do not take your own unencrypted backups of classified information.

15.5 *Virus Protection*

- Where applicable, virus protection will be installed on the device by the organisation.
- Ensure that the device is connected to the corporate network on a regular basis to allow the virus signatures to be updated.
- Do not disable virus protection on the device.

15.6 *Network Connection*

- The device should not be connected to non-corporate networks such as wireless or the Internet unless a VPN (Virtual Private Network) is used.

15.7 *Overlooking*

- When in public places, ensure that you site the device such that unauthorised people cannot view (or take photographs or video of) the screen

16 *Information Sensitivity Policy*

The Information Sensitivity Policy is intended to help staff determine what information can be disclosed to non-staffs, as well as the relative sensitivity of information that should not be disclosed outside of Fincra without authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only.

Minimal Sensitivity
General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Fincra Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Fincra Proprietary" or similar labels at the discretion of such individual business unit or department. Even if no marking is present, Fincra information is presumed to be "Fincra Confidential" unless expressly determined to be Fincra Public information by an Fincra employee with authority to do so.

Access: Fincra employees, contractors, people with a business need to know.

Distribution within Fincra: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Fincra internal mail: Nigerian mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it is sent to only approved recipients.

Storage: Keep from view of unauthorised people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Fincra premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

More Sensitive
Business, Financial, Technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Fincra Confidential" or "Fincra Proprietary", wish to label the information "Fincra Internal Use Only" or other similar labels at the discretion of such individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Fincra employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within Fincra: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Fincra internal mail: Sent via Nigeria mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within Fincra, but should be encrypted or sent via a private link to approved recipients outside of Fincra premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on Fincra premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Most Sensitive
Trade secrets & Marketing, Operational, Personnel, Financial, Source code, & Technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Fincra Confidential information is very sensitive, you may, should label the information "Fincra Internal: Registered and Restricted", "Fincra Eyes Only", "Fincra Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Fincra Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Fincra employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within Fincra: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of Fincra internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within Fincra, but it are highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Fincra premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Sensitive information requires extreme precautions to ensure the integrity and confidentiality of information (media and the underlying information assets associated with that media).

Cardholder data media and all distributed media, including that distributed to individuals, must be categorised as extremely sensitive even when masked or encrypted.

Sensitive information must be protected at all times from unauthorized use, modification or retrieval.

17 *Teleworking*

A teleworking arrangement is a voluntary agreement between the organisation and the employee. It usually involves the employee working from home in a separate area of their living accommodation, whether this is a house, apartment or other type of domestic residence.

The introduction of a teleworking arrangement, if managed effectively, has the potential to benefit both the individual and the organisation. The individual will gain greater flexibility in working arrangements and possibly avoid a lengthy commute to and from an office. The organisation is able to retain skilled and experienced staff whose circumstances suit teleworking and possibly save money on the rental, lease or purchase of office space.

This policy sets out the key information security-related elements that must be considered in agreeing a teleworking arrangement. It ensures that all of the necessary issues are addressed and that the organisation's information assets are protected.

This policy does not address the human resources aspects of teleworking such as health and safety, absence monitoring, job performance and contractual issues. These will be handled by People Operations and must also be in place before the teleworking arrangement begins.

From an information security point of view there are various aspects that need to be considered in each teleworking arrangement and the policy of the organisation in these areas is set out in the following sections.

17.1 *Initial Risk Assessment*

Before a teleworking arrangement can commence there will be an initial risk assessment of the proposed environment and nature of the work to be carried out.

17.2 *Nature of the Work*

A major part of the risk assessment concerns the type of activities that are to be carried out as part of the arrangement. A full understanding needs to be gained of:

- The classification of the information that will be stored and processed as part of the role
- The method of access of the information
- Whether the role requires that classified information is printed locally
- The business criticality of the role and the consequences if it were unavailable

17.3 Physical Security

The risk assessment will also consider the physical security of the proposed work location:

- Is there enough room to house the required equipment safely?
- Is it in a separate area of the living accommodation?
- Can the work area be secured e.g. via a locked door when not in use?
- Who else has access to the work area?
- Will the equipment be visible from outside the accommodation e.g. through a window?
- What is the likelihood of theft in the surrounding area?
- Can paper documents be locked away securely?
- Is there adequate and reliable power supply to the work area?

17.4 Insurance

The impact of teleworking on the individual's home insurance should be investigated to ensure that any policies currently in place remain valid. Additional insurance may be required and if so it should be agreed in advance how this will be funded.

17.5 Equipment

Only client equipment provided by Fincra for the purpose of teleworking may be used to access company networks. The individual's own devices such as laptops or PCs must not be used for this purpose.

According to requirements, the teleworker may be provided with:

- A laptop
- Desk and chair

This equipment remains the property of the organization at all times.

17.6 Communications

A Virtual Private Network (VPN) will be used to ensure that all network traffic from the teleworker client to organization servers is encrypted to organization standards.

17.7 Backup and Virus Protection

Where possible, no data will be stored on the client machine. In the event that this is unavoidable it is the responsibility of the teleworker to ensure it is backed up to the corporate network as soon as possible.

Virus protection will be provided on all relevant equipment and configured to update automatically on connection to the corporate network.

17.8 Technical Support

Technical support of all supplied equipment will be provided by the Information Security Unit.

17.9 Agreement Termination

In the event that the teleworking agreement is terminated for whatever reason, all equipment that was supplied as part of the arrangement must be returned to the Information Security/People Operations as soon as possible.

18 Bring Your Own Device (BYOD)

The purpose of this policy is to set out the controls that must be in place when using mobile devices that are not owned or provided by the organisation. It is intended to mitigate the following general risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of classified information through observation by the public
- Introduction of viruses and malware to the network
- Loss of reputation

It is important that the controls set out in this policy are observed at all times in the use and transport of BYOD mobile devices. It is a joint decision between the organisation and the owner of the device concerning whether any particular device will be used for business purposes. Such use is not compulsory and the employee has the right to decide whether the additional controls placed on the device by the organisation are acceptable and therefore whether they choose to use the device for business purposes.

18.1 What is BYOD?

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful the number of tasks that can be achieved away from the office grows.

Mobile devices include items such as:

- Laptop and notebook computers
- Tablet devices
- Smartphones
- PDAs

Historically, such devices have been provided by the organisation where appropriate for exclusively business use. But the low cost and general availability of such devices has fuelled the desire amongst employees and other stakeholders to use their own devices for business use. In some cases, this can provide increased flexibility and remove the need for the employee to carry more than one device on a regular basis.

However, the concept of allowing an employee to make use of their own device(s) for business purposes may result in the need for such devices to be subject to additional controls over and above those typically in place for a consumer device.

Common issues and security challenges with BYOD may include:

- use of the device by other family members
- default storage of data in cloud backup facilities
- increased exposure to potential loss in social situations e.g. on the beach, in a bar
- potential access to websites that do not meet the organisations acceptable use policy
- Connection to insecure networks e.g. unsecured wireless hotspots
- Anti-virus protection and how often the device is patched
- Installation of potentially malicious apps onto the device (often without the user being aware that they are malicious)

These issues must be considered when assessing the suitability of any given device to hold specific data belonging to the organization.

o

18.2 *BYOD Assessment Process*

Individuals must not use their own devices to hold and process company information unless they have submitted a request to do so, and that request has been formally approved. It is Fincra's policy to assess each BYOD request on an individual basis in order to establish:

- the identity of the person making the request
- the business reason for the request
- the data that will be held or processed on the device
- the specific device that will be used

Requests should be submitted to Information Security Unit.

The general principle of this policy is that the degree of control exercised by the organisation over the BYOD device will be appropriate to the sensitivity of the data held on it. The information classification scheme in use within Fincra is described in the document Fincra Information Security Classification Guidelines.

Guidance to be used in the decision regarding who should have access to what information on which device is summarised in the table on the following page.

Information category	Examples	Who may have access via BYOD	Types of BYOD devices	Required controls	Comments
Level 0 - Public	Product catalogues, pricing information, company location addresses and contact numbers	Anyone	Any	None	This information is generally available to the public and accessed via publicly-accessible means e.g. a website
Level 1 – Protected / Internal	Internal procedures, product details, internal company communications e.g. non restricted or confidential email	Employees and other approved stakeholders	Laptops (Windows 10 or later) Tablets (IOS x / Android y or later) Smartphones (Apple iPhone 8 or later)	Device password protection Inactive lock Remote wipe Application password protection Periodic audits	This area is the most likely use of BYOD within the organisation
Level 2 - Restricted	HR information, organization details, personal information covered by data protection legislation	Restricted groups of employees	Laptops only (Windows 10 or later)	Full disk encryption VPN Automated patching Anti-virus Firewall Regular audits	This information may be accessible via devices with strict security controls. This may practically preclude the use of a BYOD device depending on the circumstances
Level 3 - Confidential	Company resourcing plans, commercial proposals, unpublished financial information	No-one	None	Not applicable	This information may be accessible via organisation-provided devices with strict security controls

Table 1 – BYOD Guidance

18.3 Audit and monitoring

In order to ensure its data is adequately protected It is important for Fincra to be able to monitor and audit the level of compliance with this policy. The level of monitoring and audit will be appropriate to the classification of the information held on the device.

The methods and timing of monitoring and audit should be such that the device owner's privacy is not invaded and should be in line with applicable privacy legislation. In general, monitoring of usage outside of business hours should be avoided.

In the event of the device being lost or stolen, the owner must inform the IT service desk as soon as possible, giving details of the circumstances of the loss and the sensitivity of the business information stored on it. Fincra reserves the right to remote wipe the device where possible as a security precaution. This may involve the deletion of non-business data belonging to the device owner.

Upon leaving the organisation, the device owner must allow the device to be audited and all business-related data and applications removed.

19 Software Policy

Fincra uses many types of computer software to perform its business operations and relies upon the correct functioning and security of that software at all times. It is imperative therefore that steps are taken to ensure that only approved software is used within the organisation and that no classified information is put at risk.

This policy sets out how software will be acquired, registered, installed and developed within Fincra.

o

19.1 Purchasing Software

All computer software to be used within the organisation must be purchased through [Apple App Store. This is necessary to ensure that:

- Licensing requirements are addressed
- The software works effectively with the standard corporate software image
- Use of the software can be supported by the Information Security
- Best value for money is obtained in procurement
- A record is kept of installed software within the organisation

Under no circumstances should software be purchased using local departmental budgets.

19.2 Software Registration

All software in use within Fincra must be correctly licensed. This is a legal requirement and compliance is monitored by various industry bodies including FAST (Federation Against Software Theft).

All installed software programs will be registered in the name of the organisation, not the individual. Purchased software is a corporate asset and licences will frequently be reused as the shape of the organisation changes.

Under no circumstances will corporate software be copied (other than for backups) or installed for use on non-corporate machines, such as at home. This is against the law.

[Service Provider] will maintain a register of all licensed software within the organisation and licensed copies of media such as CDs and DVDs in a Definitive Media Library (DML). This register will include:

- Physical location
- Inventory number
- Supplier
- Software description
- Issue date
- Number of disks in set
- License key(s)
- Any other relevant information

Asset management software will be used to keep track of all installed instances of software titles and regular audits will be carried out. Any user with unlicensed software installed will be asked to remove it; it is the responsibility of users to ensure that all the software on their computer equipment is licensed.

19.3 Software Installation

Licensed software will be installed by Information Security or appropriate technical team or supplier upon request and once any required licences have been purchased.

Software will not be installed prior to a valid licence being ordered.

The user will not install any software that is licensed to them personally, whether or not it is free, shareware or commercial. This includes evaluation versions of software programs.

19.4 Removal of Software

In the event that a software program is no longer required the Information Security Unit should be informed. The software will then be removed from the machine in question and where possible the license will be re-used elsewhere within the organisation.

Users should not remove licensed software from their machines without informing the IT Service Desk as this potentially represents a waste of a corporate asset.

19.5 In-House Software Development

Fincra develops its own software for particular purposes where a commercial package is not available or does not fulfil the identified requirements. In such cases a structured development method will be used to ensure that software is developed to organisational standards and is tested and implemented in a managed way.

Alterations to in-house developed software such as the addition of fields or screen changes may be requested through the change request process. This process is described in documents Fincra Change Management Policy and Fincra Change Management Process.

Changes to in-house developed software must not be made without following the change management process.

19.6 Software Patent

1. Computer programs, source code, design details, flowcharts, documentations and other software originating from Fincra should not be copyrighted.
2. The rights to software developed by Fincra developers in the course of the developer's employment shall reside with Fincra.
3. All the organizations owned software shall bear copyright notice imbedded in the application.
4. Software program, source code, design details developed by third party vendors, should not be used for commercial purposes; it is the property of the organization and should not be used by the vendor in any form outside Fincra.
5. In house software/application and third party developers are not required to disclose source code or application program to any competitor or sold for commercial purposes.

6. Developers are not required to copy application software or source code in the event of leaving the organization. The application and source code is the property of the organization and should not be used for commercial purposes.

20 Anti-Malware Policy

The threat posed by malware has never been more serious than it is today. Fincra systems and users are under a constant bombardment of attempts to circumvent security in order to make some kind of gain or to disrupt the normal operation of the organisation.

This threat can come from a number of sources including:

- Organised gangs attempting to steal money or commit blackmail
- Competitor organisations trying to obtain confidential information
- Politically motivated groups
- Rogue employees within the organization
- Nation state sponsored "cyber-warfare" units
- Individuals exercising curiosity or testing their skills

Whatever the source, the result of a successful security breach is that the organization and its stakeholders are affected, sometimes seriously, and harm is caused.

One of the primary tools used by such attackers is malware and it is essential that effective precautions are taken by Fincra to protect itself against this threat.

20.1 Definition

There is no single definition of the term "Malware" in use but for the purposes of this policy the following definition is used:

"Malware is any code or software that may be harmful or destructive to the information processing capabilities of the organisation"

The term is derived from the phrase "Malicious Software" and may also be called malicious code or commonly (but inaccurately) "a virus".

20.2 Types of Malware

Malware comes in many forms and is constantly changing as previous attack routes are closed and new ones are found. The most common types of malware found today are:

- Virus – a program that performs an unwanted function on the infected computer. This could involve destructive actions or the collection of information that can be used by the attacker
- Trojan – a program that pretends to be legitimate code but conceals other unwanted functions. Often disguised as a game or useful utility program
- Worm – a program that is capable of copying itself onto other computers or devices without user interaction
- Logic bomb – malicious code that has been set to run at a specified date and time or when certain conditions are met
- Rootkit – a program used to disguise malicious activities on a computer by hiding the processes and files from the user
- Keylogger – code that records keystrokes entered by the user
- Backdoor – a program that allows unauthorised access at will to an attacker

Often these types of malware will be used in combination with each other. For example an attacker will encourage an unwitting user to infect a computer with a virus which will allow unauthorised access. This initial access will then be used to install a rootkit to disguise further activities, a keylogger to capture keystrokes and a backdoor to allow future access without detection.

20.3 How Malware Spreads

In order for malicious software to carry out its intended purpose it needs to be installed on the target device or computer. There are a number of key ways in which malware infects computers and networks, although new ways are being created all the time.

The most common infection techniques are as follows.

- Phishing

This method involves tricking the user into taking some action that causes a malicious program to run and infect the computer being used. It is usually achieved via the blanket sending of unsolicited emails (Spam) with file attachments or web links included in them. When the user opens the file or clicks on the link the malicious action is triggered.

Phishing attacks have become more sophisticated in recent years and can be very believable and enticing to the user. More targeted versions of phishing have appeared such as Spear Phishing (aimed at a particular organisation) and even Whaling (aimed at an individual).

- Websites and Mobile Code

The widespread use of mobile code such as JavaScript on websites has provided attackers with another route to infect computers with malware. Often websites will be created to host

the malware which is activated either upon clicking on a link or in some cases simply by visiting the website.

Increasingly, legitimate websites are being compromised and made to host malware without the owner's knowledge, making this type of attack very difficult for the user to avoid.

- Removable Media

USB memory sticks, CDs, DVDs and other removable media devices provide an effective way of spreading malware onto additional computers. When the media is inserted into the machine the malware will either run and infect the target or will copy itself onto the removable media in order to prepare to infect the next machine it is plugged into.

- Hacking

Or "Cracking" as it is more accurately known, is a more targeted and therefore less common method of introducing malware onto a computer or network by gaining unauthorised access to the network from outside (and sometimes inside) the organisation. This method requires more knowledge on the part of the perpetrator and often exploits existing vulnerabilities in the software or network devices being used. Once access has been gained, malware will be installed remotely onto the compromised machine.

20.4 Anti-Malware Approach

In order to prevent the infection of Fincra computers and networks and avoid the potentially dire consequences of such infection, there are a number of key controls that will be adopted as policy.

The key concept adopted in this policy is "defence in depth" and no single control should be relied upon to provide adequate protection. This is therefore not a choice between controls but a list of necessary controls, all of which should be implemented where possible to guard against the threats outlined in the previous section.

20.5 Firewall

A firewall will be installed at all points at which the internal network is connected to the Internet. Where possible, individual firewalls will be enabled on client computers. Access permissions should be set such that the user cannot disable the firewall.

20.6 Anti-Virus

A commercial, supported anti-virus platform will be installed within Fincra at key locations:

- Firewall

- Email servers
- Proxy servers
- All other servers
- All user computers
- Mobile devices, including laptops (phones and tablets where possible)

All antivirus clients will be set to obtain signature updates on a regular basis, either directly from the vendor website or from a central server within the organisation.

By default, on access scanning should be enabled to provide real time protection. Regular full scans should also be carried out at least once every week and quick scans should be carried out every day.

Users should not be able to disable the protection which is configured centrally.

20.7 *Spam Filtering*

A system should be installed to filter out unsolicited and potentially harmful emails (spam). Types of attachments known to often contain malware should be blocked or removed before delivery to the user.

20.8 *Software Installation and Scanning*

Users should not have sufficient administrative access to their computer to allow them to install software onto it. Only approved software should be allowed and this must be installed by the IT department upon authorised request.

Regular scanning of user computers to detect unauthorised software should be carried out.

o

20.9 *Vulnerability Management*

Information on software vulnerabilities will be collected from vendors and third party sources and updates applied where available. If possible and if permitted by the organizational change management policy, updates should be applied automatically as soon as they are released.

Vulnerability scanning should be carried out regularly, particularly on business critical servers and networks.

For new vulnerabilities identified by Fincra employees, a disclosure policy will apply.

Vulnerability is defined in NIST Special Publication 800-30 Rev 1 as "an inherent weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source."

The software development process is complicated and its output in the form of software programs is rarely bug free. Most of these bugs simply affect the functionality of the software so that it doesn't work as intended. However, if manipulated in the correct way, some can allow an attacker to gain some form of advantage or access which was not intended by the developer. This type of bug is commonly considered to be a software vulnerability.

These vulnerabilities are constantly being found and corrected via software updates or patches. Unfortunately, it is not always the developer or user who discovers these vulnerabilities. When discovered by a potential attacker, the vulnerability becomes something to be exploited for gain and kept secret for as long as possible. A newly-discovered vulnerability is often referred to as a "zero day exploit" and is difficult to defend against.

Fincra's policy with respect to technical vulnerabilities is to be aware of them and to close them where possible, either directly or via other means.

The first step in managing technical vulnerabilities is to become aware of them. Since we are talking about technical vulnerabilities, these will of course depend upon the technology employed within Fincra. It is necessary then to gain a full appreciation of the technology components that make up the organisation's infrastructure and their versions (since most technical vulnerabilities are very version-specific).

This should include:

- Operating systems e.g. UNIX, PAN OS, IOS
- Databases e.g. SQL Server, MySQL
- Web servers e.g. IIS, Apache
- Desktop software e.g. Office, Acrobat
- Web technologies e.g. Flash, Java
- Application software e.g. SAP, Agresso
- Hardware e.g. servers, routers

This information should be available from the organisation Fincra Software Catalogue.

Information about vulnerabilities with any of the above components is generally available from the vendor who will issue updates and patches to fix those that it becomes aware of.

A process should therefore be put in place to ensure that all relevant information about updates is being received and reviewed by competent staff members. This will usually give guidance about the level of urgency associated with each update.

Where configuration changes are recommended to close off vulnerabilities, these should be actioned through the organization change management process so that appropriate controls are in place for testing, risks assessment and back out.

20.10 Patches and Updates

Patches and updates will typically be issued by software vendors on a regular schedule as cumulative packages. These will be linked to the specific version of software that they relate to and may have dependencies stipulated with other software modules, products or operating systems.

Procedures should be put in place to obtain copies of the software updates electronically when they are issued by the vendor. The scheduling of the installation of updates will depend upon a number of factors including:

- The criticality of the systems being updated
- The expected time taken to install the updates (and requirements for service outages to users)
- The degree of risk associated with any vulnerabilities that are closed by the updates
- Coordination of the updating of related components of the infrastructure
- Dependencies between updates

An update release plan should be created and maintained to keep track of when various system will be updated, taking into account the factors listed above. The plan must be managed through the change management process. For updates that are low risk and regular, a standard change may be defined within the change management process to allow this to happen without excess administrative overhead (see Fincra Change Management Policy).

20.11 Vulnerability Assessment

In addition to the regular application of vendor-supplied software updates, Fincra will conduct a vulnerability assessment periodically. The focus of the vulnerability assessment should be guided by the most recent risk assessment.

The purpose of this assessment is to identify existing vulnerabilities in systems that could be exploited by an attacker. These could include known software vulnerabilities that have not been patched, configuration errors that need to be corrected or examples of inadequate security practice that need to be addressed.

The assessment may be carried out in-house, by an external company or a combination of both and as a minimum should cover:

- Assessment of the security of all routes into the organisation's internal network from the Internet
- Externally-facing web servers
- Business critical servers on the internal network
- A selection of typical user computers

If resources permit, additional areas should be assessed such as the vulnerability of employees to phishing attacks.

It is not Fincra's policy to attempt to exploit the vulnerabilities found as a matter of course. This type of penetration test may be commissioned as required using external specialist resources as part of a carefully planned exercise performed outside of normal business hours.

20.12 Hardening

A further action that should be taken to reduce the number and extent of vulnerabilities within Fincra systems is the hardening of server and other device configurations. This involves the shutting down of services and protocols that are not needed so that the attack surface is reduced.

These hardening activities should be carried out according to vendors' guidelines and under the control of the change management process.

20.13 User Awareness Training

Users should be made aware when starting with the organisation of the information security policy and be trained in ways to avoid falling victim to attacks such as phishing.

This awareness training should be repeated on a regular basis to all employees who make use of IT equipment.

20.14 Threat Monitoring and Alerts

Information about emerging threats should be obtained from appropriate sources and users alerted proactively of potential attacks, giving as much detail as possible to maximise the chance of recognition.

20.15 Technical Reviews

Regular reviews will be carried out of business critical servers and networks to identify any malware that has been installed since the last review. This will include the taking of a snapshot of the configuration for later comparison purposes.

20.16 Malware Incident Management

In the event that malware is detected on a server, client, network or other IT component, an information security incident will be raised. This will be managed in accordance with the procedures set out in Fincra Information Security Incident Management Procedure.

21 Network Security

The use of networks is an essential part of the day to day business of Fincra. Networks not only connect many of the components of business processes together internally, but they also link the organisation with its suppliers, customers, stakeholders and the outside world.

The organisation's networks have evolved over a period of time to become the circulatory system of the company, transporting information to where it needs to go and enabling business to be carried out effectively.

But the fact that so much information runs through our networks makes them a target for those who would try to steal that information and disrupt our business. Therefore these networks need to be protected to ensure that the confidentiality, integrity and availability of our vital information are assured at all times.

The effective protection of our networks requires that we adopt good practices in information security covering the design, implementation, operation and management of them and that we ensure that everyone involved follows these practices.

This policy sets out Fincra's rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure.

21.1 Network Security Design

The design of networks is a complicated process requiring a good knowledge of network principles and technology. Each design is likely to be different, based on a specific set of requirements that are established early on in the process. This policy does not attempt to specify how individual networks should be designed and built, but provides guidance for the standard building blocks that should be used.

A network design should be based on a clear definition of requirements which should include the following security-related factors:

- The classification of the information to be carried across the network and accessed through it
- A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities
- The level of trust between the different components or organisations that will be connected
- The hours of availability and degree of resilience required from the network
- The geographical spread of the network
- The security controls in place at locations from which the network will be accessed
- Security capabilities of existing computers or devices that will used for access

Requirements should be documented and agreed before design work starts.

21.2 Defence in Depth

A "Defence in Depth" approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network. For example network firewalls should be supplemented by host-based software firewalls on servers and clients in order to provide several levels of firewall protection.

At key points in the network, a "defence diversity" approach should also be taken so that vulnerabilities are minimised. For example, this may involve using firewalls from different vendors in series so that if a vulnerability is exploited in one device, the other will not be subject to it. This may be extended to the use of more than one network virus scanner at the perimeter for the same reason.

21.3 Network Segregation

The principle should be adopted that a network should consist of a set of smaller networks segregated from each other based on either trust levels or organisational boundaries (or both).

For a large network this should be achieved using separate domains, particularly where separate organisations' networks are being linked. An appropriate level of trust should be configured at the domain level and domain perimeters should be secured using a firewall where appropriate.

Within networks, Virtual Local Area Networks (VLANs) will be used to segregate organisational units.

21.4 Perimeter Security

At all perimeters between the internal network and an external network (such as the Internet) effective measures should be put in place to ensure that only authorised network traffic is permitted. This will usually consist of at least one Stateful Inspection firewall and for major links with the Internet an Application (or Application Gateway) firewall should be used. For connections such as broadband at smaller locations a Packet Filtering firewall may suffice, depending on the results of a risk assessment.

Servers that are intended to be accessed from an external, insecure network (such as web servers) should be located in a DeMilitarised Zone (DMZ) of the firewall in order to provide additional protection for the internal network.

21.5 Firewall and Routers

This Policy is intended to describe the required minimal security configuration for all Firewall, Routers and Switches connecting to a production network or used in a production capacity at or on behalf of Fincra.

The process of adding a Network Administrator will go through change management process using the approved workflow by the organisation called Integrify.

A current network diagram will be maintained which displays all connections to cardholder data, including wireless networks and showing Credit Card Databases segregated from the DMZ

Only members of the Administrator of Network Devices or their designee may install, uninstall, move, perform maintenance upon, or change configuration of a firewall or router.

Only the administrator to the Network Device or their designee may make the physical connection to the network device, including the direct access ports console ports etc.

In the event that the firewall or router suffers physical damages or there is evidence of tampering, it will be fully evaluated by hardware diagnostic and the physical configuration checked with existing documentation.

Only members of the administrators to the Network Devices or their designee may do the following:

- Log in directly to a network device
- Assume administrative privileges on a network device
- Log in to the network device remotely

This checklist will be used to review router security configurations:

- Router security policy written, approved, distributed.
- Router IOS version checked and up to date.
- Router configuration kept off-line, backed up, access to it limited.
- Router configuration is well-documented, commented.
- Router users and passwords configured and maintained.
- Password encryption in use, enable secret in use.
- Enable secret difficult to guess, knowledge of it strictly limited. (if not, change the enable secret immediately)

- Access restrictions imposed on Console, Aux, and VTYs.
- Unneeded network servers and facilities disabled.
- Necessary network services configured correctly (e.g. DNS)
- Unused interfaces and VTYs shut down or disabled.
- Risky interface services disabled.
- Port and protocol needs of the network identified and checked.
- Access lists limit traffic to identified ports and protocols.
- Access lists block reserved and inappropriate addresses.
- Static routes configured where necessary.
- Routing protocols configured to use integrity mechanisms.
- Logging enabled and log recipient hosts identified and configured.
- Router's time of day set accurately, maintained with NTP.
- Logging set to include consistent time information.
- Logs checked, reviewed, archived in accordance with local policy.
- SNMP disabled or enabled with good community strings and ACLs.

21.6 Public Networks

Where information is to be transferred over a public network such as the Internet, strong encryption via SSL must be used to ensure the confidentiality of the data transmitted.

Servers that will be accessed from devices on the public network will be located in the DMZ of the firewall.

21.7 Wireless Networks

Wireless networks should be secured using WPA2 encryption. WEP and WPA should not be used.

Wireless networks should be treated as insecure even if WPA2 is used as the encryption method and a firewall installed between the wireless network and the main LAN.

A guest wireless network may be provided for visitors. This should be physically separate from all internal networks (including internal wireless networks) and also secured using a firewall.

Wireless access points should be configured to not broadcast their SSID and to not allow secure connection using WPS (Wi-Fi Protected Setup) via physical access to the access point itself.

Wireless access point admin logon passwords should always be changed from the default.

21.8 Physical Security

Remote network equipment will be housed in secure cabinets which will be locked at all times. Only support staff will have access to the key to each cabinet.

Backbone and centralised network equipment will be housed in appropriate lockable cabinets or racks in a secure server room to which only authorised support staff will have access (with the exception of local facilities staff for reasons of health and safety).

Wireless access points located in public areas should be hidden from view where possible and should be placed in positions where access by the public is difficult e.g. in or near the ceiling. A lockable protective casing should be installed where an access point is located in an unprotected public area e.g. a car park.

21.9 Remote Access

Where there is a requirement for remote access to the internal network the following controls will be used:

- A Virtual Private Network (VPN) will be used providing session encryption using TLS
- Two factor authentication at the client where appropriate
- HIP will be used to restrict access to remote clients that do not meet minimum requirements e.g. virus control

Remote access should be granted on an "as required" basis rather than for all users by default.

Automatically disconnect sessions for remote-access technologies after a specific period of inactivity.

Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use

Any activity that may potentially compromise the organisation's network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organisation because of misuse of these remote access technologies will not be tolerated.

21.10 *Virtual Private Networks*

Where there is a requirement for Remote Access IPsec or L2TP Virtual Private Network (VPN) to connect to the Fincra corporate network, the following guidelines should be adhered to strictly

Users of computers that are not Fincra-owned equipment must configure the equipment to comply with Fincra's VPN and Network policies.

Only Palo Alto VPN clients may be used.

Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks

Ensure that only trusted keys and/or certificates are accepted.

Ensure that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.

Dual (split) tunneling is NOT permitted; only one network connection is allowed.

VPN gateways will be set up and managed by Fincra network operational group.

All computers connected to Fincra internal networks via VPN or any other technology must use the most up-to-date antivirus software that is the corporate standard; this includes personal computers.

VPN users will be automatically disconnected from Fincra's network after thirty minutes of inactivity. The user must then log on again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

Ensure that the proper encryption strength is implemented for the encryption methodology in use.

For SSL/TLS implementations:

- Ensure that HTTPS appears as a part of the browser Universal Record Locator (URL).

21.11 *Network Intrusion Detection*

A Network-based Intrusion Detection System (NIDS) should be installed at the network perimeter and at all key points within the network, e.g. on critical servers.

For networks with high security requirements, an Intrusion Prevention System (IPS) should be considered, although its implementation should be approached with caution to avoid a high degree of false positives with corresponding disruption to service to users.

21.12 Network Security Standards

The following standards will be adopted with respect to network configuration and security.

- Network Hardware

Where possible a single supplier policy will be used for network hardware. An exception will be made where the use of multiple vendor hardware may increase the level of security provided e.g. in a dual network-based firewall configuration.

Network routing will be based on Palo Alto firewall and virtual routers using OSPF. Palo Alto virtual switches will be used as standard for connectivity. Switch ports, including diagnostic ports will be configured to be administratively disabled until required. Hubs will not be used due to their inherent security weaknesses.

- IP Addressing

IPv4 will be used on internal networks. However new network devices purchased should support IPv6 in preparation for the future.

The internal IP address range used will fall within the private IP address ranges. The assignment and use of subnets should be monitored carefully.

IP addresses and associated network information for desktop and laptop clients will be controlled using DHCP. Internal DNS servers will be used.

- Network Protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate but other OSI layer 4 network protocols should not be used.

Only protocols and ports required on a specific server should be enabled by default in order to reduce the attack surface. This is especially true for servers within the DMZ of the firewall(s).

21.13 Network Security Management

Once networks have been designed and implemented based on a clear set of security requirements, there is an on-going responsibility to manage and control the secure networking environment to protect the organisation's information in systems and applications. This should be achieved via controls in the following areas.

21.14 Roles and Responsibilities

Roles and responsibilities for the management and control of networks should be clearly defined. In order to provide effective segregation of duties, the operation of networks is managed separately from the operation of the rest of the infrastructure such as servers and applications.

This segregation of duties is detailed in the following table.

Manager Role	Team	Main Responsibilities
Networks Team lead	Network and Communications Management	1. Ensure 98% availability of links and network resources. 2. Monitor overall network performance, analysis and review to ensure highly stable and predictable network infrastructure to greatly improve TAT Organisation-wide 3. Oversee network planning, design and optimization of existing infrastructure 4. Plan, monitor and control new projects/POCs 5. Ensure network capacity management by leading the development/improvement of procedures and standards for IT network infrastructure operations 6. Provide management reporting with a view to provisioning and remediating accordingly. 7. Ensure effective SLA management with vendors 8. Oversee collaborative working relationships with internal groups and units by identifying their requirements and providing adequate network solutions to meet their needs 9. Actively contribute to team budget and lead cost negotiations 10. Identify research, evaluate and recommend network related tools and emerging network Technologies which will reduce Overall Cost, create efficiencies, and Provide significant value
Server Storage and Desktop Support	Computer Operations	1. Ensure availability of the platform and other third party application infrastructure 2. Secure the organisation's investments by ensuring all Apple laptops and AWS Instances meet the require security level and utilization. 3. Reduce the cost of doing business by ensuring server resources are managed properly and are adequately utilized. 4. Ensure Messaging and Collaboration infrastructure is 99.9% available for business communication and cost reduction. 5. Oversee the Proactive monitoring of systems to ensure they are reliable, up to date and are protected

Manager Role	Team	Main Responsibilities
		from unauthorised access 6. Supervise and ensure standard compliance procedures are strictly followed 7. Ensure financial data of the organization is properly stored, timely available to requesting departments as well as confidential. 8. Evaluate and research new technologies

21.15 Logging and Monitoring

Logging levels on network devices should be configured in accordance with organisation policy (see Fincra Procedure for Monitoring the Use of IT Systems) and logs monitored on a regular basis.

Firewall logs should be monitored for signs of excessive port scanning which may be a precursor to a remote attack. Where installed, a Network-based Intrusion Detection System should be configured to alert the Network Operations team of this activity.

Network monitoring for availability should be achieved using CloudWatch and recovery actions automated where possible.

21.16 Network Changes

All changes to network devices will be subject to the change management process (see Fincra Change Management Process) and appropriate risk assessment, planning and back-out methods put in place. The Configuration Management Database (CMDB) should be updated whenever such changes are carried out so that a current and accurate picture of the network is maintained at all times.

21.17 Network Security Incidents

Events which are deemed to be network security incidents should be recorded and managed according to the incident management process (see Fincra Incident Management Process).

Major network outages should be managed via the Major Incident Management Process (see Fincra Major Incident Management Process) which provides for the invocation of aspects of the business continuity plan where appropriate.

21.18 Network Access Control

Only authorised or legitimate users should be granted access to Fincra's corporate network on a need to have basis. To achieve this, the following should serve as guidelines:

Secure protocols that may be used include; SSL, SSH, Kerberos, Https, Ftps etc.

Security banners informing all users that the system or application being accessed is proprietary, that it should be accessed only by authorized users, and that system use is monitored for enforcement purposes.

Third-party systems should be checked by the Information Security Unit to ensure that there are no threats /viruses and that the minimum security configuration requirements are met.

22 *Backups and Storage Media Handling*

22.1 *Backups*

Regular backups of essential business information must be taken to ensure that the organization can recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented. Any 3rd parties that store organisation information must also be required to ensure that the information is backed up.

Full back up documentation, including a complete record of what has been backed up must be stored along with the recovery procedure, at an off-site location in addition to the copy at the main site.

The remote backup location must be sufficiently remote to avoid being affected by any disaster that takes place at the main site.

Full documentation of the recovery procedure must be created and stored.

Regular restores / test of information from back up media must be performed to ensure the reliability of the back-up media and restore process.

o

22.2 *Storage Media*

Removable computer media (e.g. tapes, disks, cassettes and printed reports) must be protected to prevent damage, theft or unauthorised access.

Storage media being stored or transported must be protected from unauthorised access, misuse or corruption. Where couriers are required a list of reliable and trusted couriers should be established.

System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by [Service Provider] or any other departmental IT staff. (This does not include generic manuals that have been supplied with software).

Appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

If appropriate, physical controls such as encryption or special locked containers should also be used.

Storage media that is no longer required must be disposed of safely and securely to avoid data leakage.

Effective version control should be applied to all documentation and documentation storage.

Backup or storage tapes should be retained for seven (7) years in line with CBN directives.

23 Physical Security

23.1 Secure Areas

Sensitive information must be stored securely. A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there.

These could include, but are not restricted to, the following:

- Alarms fitted and activated outside working hours
- Window and door locks
- Window bars on lower floor levels
- Access control mechanisms fitted to all accessible doors (where codes are utilised they should be regularly changed and known only to those people authorised to access the area/building)
- CCTV cameras

- Staffed reception area
- Protection against damage - e.g. fire, flood, vandalism

Staff working in secure areas should challenge anyone not wearing a badge.

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by persons authorised to access those areas and should not be loaned/provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge.

An organization employee must monitor all visitors accessing secure areas at all times.

Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally by the [Service Provider] as appropriate.

Where breaches do occur, or a member of staff leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the staff member and any door/access codes should be changed immediately.

o

23.2 Paper and Equipment Security

Paper based (or similar non-electronic) information must be assigned an owner and a classification. If it is classified as sensitive, information security controls to protect it must be put in place.

Paper in an open office must be protected by the controls for the building and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area protected by access controls

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust and vibration
- Limit the risk of theft – e.g. if necessary items such as laptops should be physically attached to the desk

- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people

Data should be stored on network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the data centre must be sited in a physically secure environment.

Business critical systems should be protected by an Uninterruptible Power Supply (UPS) to reduce the operating system and data corruption risk from power failures.

All items of equipment must be recorded on an inventory, both on the Departmental and the [Service Provider] inventory. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of.

All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the departmental and the IT inventories. Cables that carry data or support key information services must be protected from interception or damage.

Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas.

o

23.3 Equipment Lifecycle Management

Service Provider and 3rd party suppliers must ensure that all of Fincra's IT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order.

Staff involved with maintenance should:

- Retain all copies of manufacturer's instructions
- Identify recommended service intervals and specifications
- Enable a call-out process in event of failure
- Ensure only authorised technicians complete any work on the equipment
- Record details of all remedial work carried out
- Identify any insurance requirements
- Record details of faults incurred and actions required

A service history record of equipment should be maintained so that when equipment becomes older decisions can be made regarding the appropriate time for it to be replaced.

Equipment maintenance must be in accordance with the manufacturer's instructions. This must be documented and available for support staff to use when arranging repairs.

The use of equipment off-site must be formally approved by the user's line manager.

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organization (e.g. returned under a leasing agreement) the data removal must be achieved by using professional data removing software tools.

Software media or services must be destroyed to avoid the possibility of inappropriate usage that could break the terms and conditions of the licences held.

Equipment deliveries must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note. Actual assets received must be recorded.

Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.

Subsequent removal of equipment should be via a formal, auditable process.

There should be a duty to audit information security arrangements regularly to provide an independent appraisal and recommend security improvements where necessary.

24 *Cryptographic Policy*

A key component in the set of controls available to organizations to protect their classified information is the use of cryptographic techniques to "scramble" data so that it cannot be accessed without knowledge of a key.

Cryptographic controls can be used to achieve a number of information security-related objectives, including:

- **Confidentiality** – ensuring that information cannot be read by unauthorised persons
- **Integrity** – proving that data has not been altered in transit or whilst stored
- **Authentication** – proving the identity of an entity requesting access to resources
- **Non- repudiation** – proving that an event did or did not occur or that a message was sent by an individual

The need for cryptographic controls will be highlighted from the Fincra risk assessment and will obviously not be applicable in all cases. However where their use can provide the required level of protection they should be applied according to the provisions set out in this policy.

In order to identify those areas in which the deployment of cryptographic techniques will be useful, Fincra will take a managed approach as follows.

24.1 Risk Assessment

The first step will be to undertake a risk assessment in line with the ISO/IEC 27001 Information Security standard. For each of the information assets identified within the organization, possible threats will be assessed together with their likelihood and impact should they occur.

The following documents within the Fincra Information Security Management System set out how this is achieved:

- Fincra Risk Assessment and Treatment Process
- Fincra Information Security Risk Assessment Report
- Fincra Information Security Risk Treatment Plan

Requirements for the use of cryptographic techniques will be identified in the last of these documents. This risk treatment plan will show in overview where cryptographic techniques should be applied and in what form to achieve the level of protection needed.

In general terms, the use of cryptography will tend to be applicable in the protection of information classified within the organization as "Restricted" or "Confidential" (see Fincra Information Security Classification Guidelines).

In addition, cryptography should be seriously considered in the following scenarios:

- On mobile devices such as laptops and Smartphones
- For authorised use of removable media such as USB memory sticks
- Where classified data is transmitted across communications lines that extend beyond the boundaries of the organization e.g. over the Internet

24.2 Technique Selection

Once the general need for the use of cryptography has been identified by the risk assessment, a decision needs to be made about which specific techniques will be deployed.

This will also involve the selection and possible purchase of software or hardware in order to implement the technique.

Note that the selection of such techniques must take into account any current regulations or national restrictions on the procurement and use of cryptographic technology. These are currently

- Payment Card Industry Data Security Standard requirement 3 and 4

These may affect the type, strength and quality of the encryption algorithm used.

In general the policy of Fincra is to use the following techniques for the relevant business process or situation:

Process/Situation	Technique	Specific Guidance
E-Commerce transactions over the Internet	Symmetric encryption using SSL/TLS (Asymmetric techniques used to share session key)	RSA to be used for public key cryptography. Certificates to be obtained from Symantec, GoDaddy, Symantec, Digicert or any reputable vendor
Protection of data on Google drive	Symmetric encryption using Virtru	AES-256 encryption to be used where available
Protection of passwords on systems	All passwords must be hashed	SHA1 and SHA2 hashing to be used where available
Email Security	Symmetric/asymmetric encryption using S/MIME	Features available in Gmail should be used to simplify the process
Remote Access	Virtual Private Network (VPN) using SSL	An IPSec VPN may be used where permitted by the Network Security Policy

The continued use of the specified techniques will be evaluated on each review of this policy.

24.3 Deployment

The deployment of cryptographic techniques must be managed carefully to ensure that the desired level of security is in fact achieved. Where possible, more than one member of staff should be closely involved in the deployment in order to avoid both a single point of failure for support and to allow segregation of duties to take place.

Close consideration should be given to the on-going operation of the installed encryption so that documented operational procedures are fully in place and the relevant staffs are trained in them.

24.4 Testing and Review

Once deployed, it is critical that the security of the encryption be tested under realistic conditions in order to identify any weaknesses. Such testing should cover the use of:

- commonly-available software tools to try to break the encryption
- social engineering methods to try to discover the key
- interception of encrypted data at various points in its transmission

The results of tests will be formally reviewed and lessons learned will be applied to the tested situation and communicated to other areas in which encryption are used in the organisation.

24.5 Key Management

It is vital that cryptographic keys are protected from modification, loss, destruction and unauthorised disclosure. A lifecycle approach will be taken to key management which will require the creation of specific procedures to cover the following stages:

- Key generation
- Distribution of keys to point of use
- Storage at point of use
- Backup as protection against loss
- Recovery in the event of loss
- Updating keys once expired
- Revoking if compromised
- Archiving once expired
- Destroying when no longer required
- Logging and auditing of key management related activities

These procedures will take account of the specific circumstances in which encryption will be used.

In principle, private asymmetric keys and symmetric keys shall only exist in the following secure forms:

1. As clear text within the memory of a hardware-based encryption device
2. As cipher text outside the memory of a hardware-based encryption device
3. As two or more key fragments either in clear text or cipher text, managed using dual control with split knowledge

Use of one of these three forms will ensure that the confidentiality of private asymmetric and symmetric keys is maintained at all times.

Public asymmetric keys are generally available and so do not require protection. Their integrity and authenticity does however need to be protected and this should be achieved via the use of a signature from a reputable Certification Authority.

In the event that cryptographic keys are subject to a request by a government agency, Fincra will comply with all legally authorised requests in a timely manner. The compliance process will be subject to senior management oversight and control.

25 Encryption Policy

Fincra ensures that customer data are protected are all times. This will be communicated to all Application Development, Network Devices and system component custodians to ensure compliance.

s/n	Component	Application Protocol	Network Protocol	Algorithm	Key Length(min)
1	Web Applications	TLS 1.2	-	AES	256 bit
2	Remote 3rd Party Connection	-	VPN IPSEC 256	VPN AES	256 bit
3	Remote connection on Windows Server	-	FIPS 140-2	AES	256 bit
4	Hard disk Encryption	-	-	AES	256bit
5	Data Transfer (e.g file upload to third party)	-	sftp	-	-
6	File/folder encryption	-	-	AES	256bit
7	Full Disk Encryption	-	-	AES	256bit

Fincra's key length requirements will be reviewed and upgraded as technology allows. If encryption is not used, then Fincra will ensure that the PAN is protected by other acceptable means such as hashing, truncating or indexing of tokens and pads.

Key-management procedures are implemented to require secure key distribution and storage.
Access to cryptographic keys is restricted to the fewest number of custodians necessary.

Cryptographic keys are stored in encrypted format and the key-encrypting keys are stored separately from data-encrypting keys.

Keys are stored in the fewest possible locations and forms

Key-management procedures are implemented to require split knowledge and dual control of keys for any manual clear-text key-management procedures, such as requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key.

The need for one or more encryption solutions in an organizationing sector setting is indisputable for all but the very smallest of entities. There are several situations where encryption may be, and probably is, necessary:

- Data at rest
  - Laptops
  - Smartphones
  - CDs / DVDs / Tapes
  - Workstations / Servers
  - iPods, Thumb drives, etc.

- Data in transit
  - Email
  - Data Transfer
  - Remote Access

Of these, several are relatively easy and inexpensive to implement, and for smaller organizations a single solution may provide security in multiple areas. For example, installing PGP may allow you to do full disk encryption on laptops, create encrypted-compressed files for transfer, and send / receive encrypted emails as well. As the size and/or complexity of the environment increases, so does the difficulty and cost of implementing controls.

26 Privacy

26.1.1 Data Protection and Privacy Statement

INSERT PRIVACY STATEMENT

26.1.2 Cookies

This website, along with most other major websites, uses cookies. Cookies are pieces of information that a website transfers to the cookie file on your computer's hard disk. Cookies enable users to navigate around the website and (where appropriate) enable us to tailor the content to fit the needs of visitors who have accessed the site.
Fincra uses two types of cookies on this website:

1. Session cookies, which are temporary cookies that remain in the cookie file of your computer until you close your browser (at which point they are deleted).
2. Persistent or stored cookies that remain permanently on the cookie file of your computer.

Cookies cannot look into your computer and obtain information about you or your family or read any material kept on your hard drive and, unless you have logged onto an authenticated page, cookies cannot be used to identify who you are.
Cookies cannot be used by anyone else who has access to the computer to find out anything about you, other than the fact that someone using the computer has visited a certain website. Cookies do not in any way compromise the security of your computer.
Cookies will not be used to contact you for marketing purposes other than by means of advertisements offered within this website.

Cookies may be used to record details of pages relating to particular products and services that you have visited on this website. This is to provide firstcitygroup.com with generic usage statistics to allow the company to improve this website and to provide you with information that may interest you.
The web browsers of most computers are initially set up to accept cookies. If you prefer, you can set your web browser to disable cookies or to inform you when a website is attempting to add a cookie. You can also delete cookies that have previously been added to your computer's cookie file.
You can set your browser to disable persistent cookies and/or session cookies but if you disable session cookies, although you will be able to view this website's unsecured pages, you may not be able to log onto any authenticated pages.
Please visit http://www.allaboutcookies.org/manage-cookies/ to discover how to disable and delete cookies.

26.1.3 Disclosures

We may divulge individual data to any individual performing review, lawful, operational, or different services for us. We will utilize data which does not identify the person for these exercises at whatever point achievable. Data divulged to vendors or contractors for operational purposes may not be re-disclosed to others by such a vendor or contractor. We may reveal individual data when needed to do as such by a court request, or court order. We may divulge individual data as we esteem it proper to secure the wellbeing of our customers or for an investigation identified with open security or to report an action that has all the earmarks of being disregarding law. We may divulge individual data to ensure the security and dependability of this site and to take safety measures against accountability.

26.1.4 Disclosures to Third Parties

Data about you that is accessible to you by means of Fincra.com, including your personal data, can become subject to the legal systems and laws in force in the country where the data is held, received or stored by you or us. Such data can become subject to disclosure pursuant to the laws of the country.
We may reveal your name and other personal data and other monetary data about you at the request of regulatory agency or in connection with an examination of us as a organization. This information could be revealed to internal and external attorneys or auditors, and to others whom we are required to make such revelations.

26.1.5 Data Protection on the Internet

At Fincra we utilize encryption innovation to ensure the transmission of data to or from you by means of Fincra.com. For security reasons and to protect the security of your information, access to Fincra.com is restricted to authorized users only. However, because information about you, your account data and other transactions can be accessed through a

public network, the Internet, there can be no guarantee that your account information will remain secure and you accept the risk that unauthorized persons may view such information. If you believe that an unauthorised person has accessed your information, please contact the Organisation immediately.

27 Cloud Usage Policy

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft, unauthorized access to corporate networks, and so on.

This cloud computing policy is meant to ensure that cloud services are NOT used without the Chief Information Officer's knowledge. It is imperative that employees do NOT open cloud service accounts or enter into cloud service contracts for the storage, manipulation or exchange of company-related communications or company-owned data without the CISO's input. This is necessary to protect the integrity and confidentiality of Fincra's data and the security of the corporate network.

Fincra's IT department remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby Fincra's employees can use cloud services without jeopardizing company data and computing resources.

27.1 Scope

This policy applies to all employees in all departments of Fincra and pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

If you are not sure whether a service is cloud-based or not, please contact the IT department.

27.2 Policy

- Use of cloud computing services for work purposes must be formally authorized by CISO. The CISO will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved.
- The use of such services must comply with Fincra's existing Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy/BYOD Policy.
- Employees must not share log-in credentials with co-workers.
- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by Fincra.
- CISO decides the information to be hosted in the cloud.

- Personal cloud service accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

27.3 Pre-approved cloud computing services

The following are the pre-approved cloud services presently being used by the organization both on office devices or personal devices such as PDAs and Mobile Phones;

1. E-mail services
2. Dashlane
3. Google Online
4. Anti-Phishing Services
5. Anti-Spam Services