Plot 97 Bukoto Street, Kampala Uganda +256 774 638 790 | +256 393 238 278 www.fltug.com | info.fltug.com

FUTURE LINK TECHNOLOGIES LIMITED

INFORMATION SECURITY POSITIONING

1. Introduction

FutureLink Technologies (FLT) is a Fintech that democratises Africa's financial services through a community-driven marketplace, so that all may thrive. We enable end consumers to efficiently access and choose the most relevant and affordable financial services provided by a growing network of Credit Unions in Africa.

Security is a key component in our offerings, and is reflected in our people, process, and products. This document is a summary of our policies related to Organizational security, Physical security, Infrastructure security, data security, operational security, Incident Management, Responsible Disclosures, Vendor Management and Customer Controls for information security assurance.

2. Organizational security

We have an Information Security Management System (ISMS) in place which takes into account our security objectives, risks and mitigation measures concerning all the interested parties. We employ strict policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data.

2.1 Employee Background checks

Each employee undergoes a process of background verification. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

2.2 Security Awareness

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles.

We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

2.3 Dedicated Security and Privacy Teams

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They engineer and maintain our defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

2.4 Internal Audit and Compliance

We have a dedicated compliance team to review procedures and policies in FLT to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards. This team also does periodic internal audits and facilitates independent audits and assessments by third parties.

2.5 Endpoint Security

All workstations issued to FLT employees run up-to-date OS version and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by FLT's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

3.0 Physical security

3.1 At workplace

We control access to our resources (buildings, infrastructure and facilities), where accessing includes consumption, entry, and utilization, with the help of access cards and biometrics. We provide employees, contractors, vendors, and visitors with different access cards that only allow access strictly specific to the purpose of their entrance into the premises. Human Resource (HR) team establishes and maintains the purposes specific to roles. We maintain access logs to spot and address anomalies.

3.2 At Data Centers

At our Data Centers, we take responsibility of the building, cooling, power, and physical security, and provide the servers and storage. Access to the Data Centers is restricted to a small group of authorized personnel. Any other access is raised as a ticket and allowed only after the approval of respective managers. Additional biometric authentication are required to enter the premises. Access logs, activity records, and camera footage are available in case an incident occurs.

3.3 Monitoring

We monitor all entry and exit movements throughout our premises in all our business centers and data centers through CCTV cameras deployed according to local regulations. Back-up footage is available up to a certain period, depending on the requirements for that location.

4.0 Infrastructure security

4.1 Network Security

Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We use firewalls to prevent our network from unauthorized access and undesirable traffic. Our systems are segmented into separate networks to protect sensitive data. Systems

supporting testing and development activities are hosted in a separate network from systems supporting FLT's production infrastructure.

We monitor firewall access with a strict, regular schedule. A network engineer reviews all changes made to the firewall everyday. Additionally, these changes are reviewed every three months to update and revise the rules. Our dedicated Network Operations Center team monitors the infrastructure and applications for any discrepancies or suspicious activities. All crucial parameters are continuously monitored using our proprietary tool and notifications are triggered in any instance of abnormal or suspicious activities in our production environment.

4.2 Network Redundancy

All the components of our platform are redundant. We use a distributed grid architecture to shield our system and services from the effects of possible server failures. If there's a server failure, users can carry on as usual because their data and FLT services will still be available to them.

We additionally use multiple switches, routers, and security gateways to ensure device-level redundancy. This prevents single-point failures in the internal network.

4.3 DDOS Prevention

We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our platforms applications, websites, and APIs highly available and performing.

4.4 Server Hardening

All servers provisioned for development and testing activities are hardened (by disabling unused ports and accounts, removing default passwords, etc.). The base Operating System (OS) image has server hardening built into it, and this OS image is provisioned in the servers, to ensure consistency across servers.

4.5 Intrusion Detection and Prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

5.0 Data security

5.1 Secure by Design

Every change and new feature is governed by a change management policy to ensure all application changes are authorized before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our code analyzer tools, vulnerability scanners, and manual review processes.

Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection,Cross site scripting and application layer DOS attacks.

5.2 Data Isolation

Our framework distributes and maintains the cloud space for our customers. Each customer's service data is logically separated from other customers' data using a set of secure protocols in the framework. This ensures that no customer's service data becomes accessible to another customer.

The service data is stored on our servers when you use our services. Your data is owned by you, and not by FLT. We do not share this data with any third-party without your consent.

5.3 Encryption

In transit: All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We mandate all connections to our servers use Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers, for all connections including web access, API access, our mobile apps, and IMAP/POP/SMTP email client access. This ensures a secure connection by allowing the authentication of both parties involved in the connection, and by encrypting data to be transferred. Additionally for email, our services leverages opportunistic TLS by default. TLS encrypts and delivers email securely, mitigating eavesdropping between mail servers where peer services support this protocol.

We have full support for Perfect Forward Secrecy (PFS) with our encrypted connections, which ensures that even if we were somehow compromised in the future, no previous communication could be decrypted. We have enabled HTTP Strict Transport Security header (HSTS) to all our web connections. This tells all modern browsers to only connect to us over an encrypted connection, even if you type a URL to an insecure page at our site. Additionally, on the web we flag all our authentication cookies as secure.

At rest: Sensitive customer data at rest is encrypted using 256-bit Advanced Encryption Standard (AES). The data that is encrypted at rest varies with the services you opt for. We own and maintain the keys using our in-house Key Management Service (KMS). We provide additional layers of security

by encrypting the data encryption keys using master keys. The master keys and data encryption keys are physically separated and stored in different servers with limited access.

5.4 Data Retention and Disposal

We hold the data in your account as long as you choose to use FLT Services. Once you terminate your FLT user account, your data will get deleted from the active database during the next clean-up that occurs once every 6 months. The data deleted from the active database will be deleted from backups after 3 months. In case of your unpaid account being inactive for a continuous period of 120 days, we reserve the right to terminate it after giving you prior notice and option to back-up your data.

A verified and authorized vendor carries out the disposal of unusable devices. Until such time, we categorize and store them in a secure location. Any information contained inside the devices is formatted before disposal. We degauss failed hard drives and then physically destroy them using a shredder. We crypto-erase and shred failed Solid State Devices (SSDs).

6.0 Identity and Access control

6.1 Single sign-on (SSO)

FLT offers single sign-on (SSO) that lets users access multiple services using the same sign-in page and authentication credentials. When you sign in to any FLT service, it happens only through our integrated Identity and Access Management (IAM) service. We also support SAML for single sign-on that makes it possible for customers to integrate their company's identity provider like LDAP,ADFS when they login to FLT services

SSO simplifies login process,ensures compliance, provides effective access control and reporting, and reduces risk of password fatigue, and hence weak passwords.

6.2 Multi-Factor authentication

FLT provides an extra layer of security by demanding an additional verification that the user must possess, in addition to the password. This can greatly reduce the risk of unauthorized access if a user's password is compromised. Currently, different modes like biometric Touch ID or Face ID, Push Notification, QR code, and Time-based OTP are supported.

6.3 Administrative Access

We employ technical access controls and internal policies to prohibit employees from arbitrarily accessing user data. We adhere to the principles of least privilege and role-based permissions to minimize the risk of data exposure.

Access to production environments is maintained by a central directory and authenticated using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Furthermore, we facilitate such access through a separate network with stricter rules and hardened devices. Additionally, we log all the operations and audit them periodically.

7.0 Operational security

7.1 Logging and Monitoring

We monitor and analyze information gathered from services, internal traffic in our network, and usage of devices and terminals. We record this information in the form of event logs, audit logs, fault logs, administrator logs, and operator logs. These logs are automatically monitored and analyzed to a reasonable extent that helps us identify anomalies such as unusual activity in employees' accounts or attempts to access customer data. We store these logs in a secure server isolated from full system access, to manage access control centrally and ensure availability.

Detailed audit logging covering all update and delete operations performed by the user are available to the customers in every FLT service.

7.2 Vulnerability Management

We have a dedicated vulnerability management process that actively scans for security threats using a combination of certified third-party scanning tools and in-house tools, and with automated and manual penetration testing efforts. Furthermore, our security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to spot security incidents that might affect the company's infrastructure.

Once we identify a vulnerability requiring remediation, it is logged, prioritized according to the severity, and assigned to an owner. We further identify the associated risks and track the vulnerability until it is closed by either patching the vulnerable systems or applying relevant controls.

7.3 Malware and Spam Protection

We scan all user files using our automated scanning system that's designed to stop malware from being spread through FLT's ecosystem. Our custom anti-malware engine receives regular updates from external threat intelligence sources and scans files against blacklisted signatures and malicious patterns. Furthermore, our proprietary detection engine bundled with machine learning techniques, ensures customer data is protected from malware.

FLT supports Domain-based Message Authentication, Reporting, and Conformance (DMARC) as a way to prevent spam. DMARC uses Sender Policy Framework (SPF) and Domain Key Identification Mail (DKIM) to verify that messages are authentic. We also use our proprietary detection engine for identifying abuse of FLT services like phishing and spam activities. Additionally, we have a dedicated anti-spam team to monitor the signals from the software and handle abuse complaints.

7.4 Backup

We run daily full backups of our databases using FLT Admin Console (ZAC) for FLT's Data Centres (DCs). Backup data in the DC is stored in the same location and encrypted using AES-256 bit algorithm. We store them in tar.gz format. All backed up data are retained for a period of three months. If a customer requests for data recovery within the retention period, we will restore their data

and provide secure access to it. The timeline for data restoration depends on the size of the data and the complexity involved.

To ensure the safety of the backed-up data, we use a redundant array of independent disks (RAID) in the backup servers. All backups are scheduled and tracked regularly. In case of a failure, a re-run is initiated and is fixed immediately. The integrity and validation checks of the full backups are done automatically by the ZAC tool.

We provide tools for all our partner institutions to regularly schedule backups of their data and exporting them from from the respective FLT services and storing it locally in their infrastructure. Although we do sufficient backupa, we strongly recommend all our partner institutions to daily export their backups to their respective storage devices.

7.5 Disaster Recovery and Business Continuity

Application data is stored on resilient storage that is replicated across data centers. Data in the primary DC is replicated in the secondary in near real time. In case of failure of the primary DC, secondary DC takes over and the operations are carried on smoothly with minimal or no loss of time. Both the centers are equipped with multiple ISPs.

We have power back-up, temperature control systems and fire-prevention systems as physical measures to ensure business continuity. These measures help us achieve resilience. In addition to the redundancy of data, we have a business continuity plan for our major operations such as support and infrastructure management.

8.0 Incident Management

8.1 Reporting

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will identify, collect, acquire and provide you with necessary evidence in the form of application and audit logs regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations.

We respond to the security or privacy incidents you report to us through privacy@fltug.com , with high priority. For general incidents, we will notify users through our blogs, forums, and social media. For incidents specific to an individual user or an organization, we will notify the concerned party through email (using their primary email address of the Organisation administrator registered with us).

8.2 Breach Notification

As data controllers, we notify the concerned Data Protection Authority of a breach within 72 hours after we become aware of it, according to the General Data Protection Regulation (GDPR). Depending on specific requirements, we notify the customers too, when necessary. As data processors, we inform the concerned data controllers without undue delay.

9. Responsible Disclosures

A vulnerability reporting program in "Bug Bounty", to reach the community of researchers, is in place, which recognizes and rewards the work of security researchers. We are committed to working with the community to verify, reproduce, respond and implement appropriate solutions for the reported vulnerabilities.

If you happen to find any, please submit the issues at www.fltug.com. If you want to directly report vulnerabilities to us, mail us at info@fltug.com

10. Vendor and Third-party supplier management

We evaluate and qualify our vendors based on our vendor management policy. We onboard new vendors after understanding their processes for delivering us service, and performing risk assessments. We take appropriate steps to ensure our security stance is maintained by establishing agreements that require the vendors to adhere to confidentiality, availability, and integrity commitments we have made to our customers. We monitor the effective operation of the organization's process and security measures by conducting periodic reviews of their controls.

11. Customer controls for security

So far, we have discussed what we do to offer security on various fronts to our customers. Here are the things that you as a customer can do to ensure security from your end:

Choose a unique, strong password and protect it.

- Use multi-factor authentication
- Use the latest browser versions, mobile OS and updated mobile applications to ensure they are patched against vulnerabilities and to use latest security features
- Exercise reasonable precautions while sharing data from our cloud environment.
- Classify your information into personal or sensitive and label them accordingly.
- Monitor devices linked to your account, active web sessions, and third-party access to spot anomalies in activities on your account, and manage roles and privileges to your account.
- Be aware of phishing and malware threats by looking out for unfamiliar emails, websites, and links that may exploit your sensitive information by impersonating FLT or other services you trust.

Conclusion

Security of your data is your right and a never-ending mission of FLT. We will continue to work hard to keep your data secure, like we always have.