GOBANKME TECHNOLOGIES SECURITY POLICY STATEMENT

1. Objective

Information is a principal asset of GoBankMe Technologies Pte Limited ("the Company", "GoBankMe", "We") and as such appropriate measures must be employed to protect this valuable asset and ensure against unauthorised modification, disclosure or destruction.

2. Scope

This policy applies to all information in the possession of the Company whether held on computer systems or otherwise. The policy is applicable to all personnel employed or working with the Company, regardless of their position, location or relationship with the Company.

3. Policy Statement

It is the Company's policy to ensure that:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Regulatory and legislative requirements will be met;
- Continuity plans will be produced, tested and maintained;
- Information security awareness among all staff will be created;
- All breaches of information security, actual or suspected, will be reported to, and investigated by the person or persons responsible for security;
- Copyright of intellectual property will be respected;
- Information Security Policies are reviewed and/or updated on a yearly basis; and
- Information will be protected against malicious code.

4. Responsibilities

GoBankMe's Information Security Officer, as the person in charge of Information Security within the Company, is responsible for maintaining the policy and providing advice on information security and guidance on its implementation.

The Board of Directors are responsible for ensuring this policy is implemented across the business areas and to ensure that all employees and partners understand their obligation to protect the Company's assets and comply with security standards and related procedures. These include, but are not limited to, ensuring that:

1. All employees understand that they have a responsibility to conduct themselves in an ethical manner;
2. Data/information obtained inappropriately should not be used;
3. Finding a system weakness is not a licence to take advantage of it;
4. Every user has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the Company's computer systems;
5. When the confidentiality of information is unclear, its classification should be ascertained;
6. Report any known violation or system weakness to the person or persons responsible for Company's security or to your line manager; and

7. All intrusions should be reported, investigated and the Incident Response Policy should be adhered to.

5. Enforcement

Non-compliance with this Policy will be subject to review and action in conformance with the Company's disciplinary procedures.

6. Standard

Other related policies, all supporting standards, procedures, guidelines, operating instructions issued in support of this policy statement, will form an integral part of this Corporate Information Security Policy Statement and shall serve as a standard to be applied by the Management. It can also serve as a basis of compliance monitoring and review.

7. Compliance

All information held or processed by the Company, that is not publicly available should be kept internal and undisclosed. Consequently, any breach of secrecy is a definite breach of the Company's policy.

Electronic communications and use of computer equipment are governed by the Computer Misuse legislation. Personal data is protected by the specific regulatory requirements of the jurisdictions in which GoBankMe Technologies and its subsidiaries are incorporated.

<u>Acceptable Use Policy</u>

The Company's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to established culture of openness, trust and integrity. GoBankMe Technologies is committed to protect its employees, partners, Account Holders and the Company itself from illegal or damaging actions by individuals, either knowingly or unknowingly carried out.

Internet related systems, including but not limited to server equipment, software, operating systems, storage media, and any documentation are the property of the Company.

1. Purpose

The purpose of this policy is to outline the general acceptable use of server equipment and documentation in the Company. These rules are in place to protect the employee, the Account Holders and the Company (including its outsourced partners). Inappropriate usage will expose the Company to risks such as virus attacks, compromise of network systems and services, and legal issues.

2. Scope

This policy applies to employees, users' contractors, consultants and part-timers, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company, the services that run on it and any documentation relevant to the equipment, products, services, clients, partnerships and Company's business.

3. General Use and Ownership

- Whilst it is the Company's desire to provide a reasonable level of privacy, users should understand that the data they create on the Company's systems remains the property of the Company.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Other policies, namely the Internet Usage Policy, should serve as a more detailed guide on personal use.
- Management recommends that any information that users consider sensitive or vulnerable be encrypted or, at a minimum, should be password protected.
- Credit/debit Card Data should always be encrypted during storage and, unless required for business reasons, masked or truncated when displayed on screen.
- For security and network maintenance purposes, authorised individuals within the Company may monitor equipment, systems and network traffic at any time.
- The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- Any documentation, inclusive of reports, is also the property of the Company and should be handled appropriately.

4. Security and Proprietary Information

Information contained on Internet systems should be classified as specified from time to time by management. Examples of confidential information include, but are not limited to:

1. the Company's corporate strategies;
2. competitor sensitive data;
3. trade secrets;
4. specifications;
5. credit/debit card data;
6. customer lists; and
7. research data.

Employees should take all necessary steps to prevent unauthorised access to this information through the following guidelines:

1. Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts.
2. Use encryption of information when a password is not deemed sufficient protection for the data. Secure encryption algorithms should be used and proper key management procedures are to be followed, where applicable.
3. Reports and documents containing sensitive or confidential information should not be left on desks or in areas accessible to unauthorised users. Employees must lock away any such documentation when they are not directly in control of it. At the end of the day all other documents should be cleared off the desks and stored away appropriately.
4. All hosts used by the employee that are connected to the Company Internet, whether owned by the employee or the Company, shall be continually executing approved virus-scanning software with an updated virus database.
5. Unless overridden by departmental or group policy.
6. Prohibited opening email attachments received from unknown senders because they may contain viruses, phishing letters and/or Trojan code.

5. Unacceptable Use

The items listed in Section 6 are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances are employees of the Company authorised to engage in any activity that is illegal under local or international law while utilising Company-owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

6. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or companies protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Company or authorised for use by the Company.
- Unauthorised copying of copyrighted material and the installation of any copyrighted software for which the Company or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms,
- Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- The transfer of sensitive data between office equipment and home equipment is prohibited without management authorisation.
- Using Company computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from Company account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:
    - accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, flooding, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior approval is

obtained from management.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Purposely circumventing user authentication or security of any host, network or account. This includes granting access to anyone who should not have access.
- Utilising technology which is not expressly approved by the Company or which is not authorised to be used in certain locations.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.
- Providing information about, or lists of, Company employees or Account Holders to parties outside the Company.
- Making copies of sensitive data, irrespective of whether it is intended for Company use.
- Reporting security incidents.

7. Compliance

Any individual found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

<u>Email Policy</u>

The Company’s critical services (that located in the protected network segment) are logically separated from the mail service.

The email service does not belong to the critical system and is never used for the transfer of card data, passwords or other limited information.

<u>Internet Security & Usage Policy</u>

This document outlines the Company’s policy on employee responsibilities for internet usage over the Company’s network.

1. Purpose

   The purpose of providing employees with access to the Internet is to conduct the required day-to-day business of the Company.

2. Ownership

   The components are property of the Company.

   The software is property of the Company.

   Any data saved on the components, devices, media or network is property of the Company.

3. Usage Policy

   All employees who require access to Internet services must do so by using the Company’s approved software and Internet channels.

   Access to illicit sites, hackers' sites or sites of a dubious nature is strictly prohibited.

   Downloading of any software or executable files is strictly prohibited.

   Users of the internet are reminded that Web browsers leave "footprints" providing a trail of all sites visited.

   Technicians who need access to certain sites of a dubious nature to monitor for security holes or system vulnerabilities or other security related exercises must

obtain specific permission to do so. Such access will be carried out from systems that do not contain sensitive data and the technician must at all times exert the utmost caution.

4. Non-Business Browsing

Any such browsing can take place during breaks; however, the usage rules above will still be applicable.

5. Compliance

Violations of this policy will result in disciplinary action, any measures up to and including termination of employment and/or legal action if warranted.

Employees noticing any violations of this policy are to report them immediately to the person responsible for Information Security. The identity of any employee reporting a violation will be kept confidential at all times.

User Management Policy and Standards

1. Objectives

User Management control is implemented within the Company's systems to achieve two controls:

1. preventing intruders from entering the system; and,
2. limiting authorised users to their legitimate purposes.

2. Scope

This policy applies to all employees, users, contractors, Account Holders and any other party requiring access to Company data or systems wherever they are located or whatever form or shape they may take.

3. Control of Entry to a System

This will be achieved by requiring the would-be user to log-on to the system by entering a User ID or User Name recognisable by the system and then a password or passphrase to confirm that he is the legitimate owner of the User ID. Users should not be allowed to communicate with the system in any way before completing log-on. Identification A User ID most often consists of a non-secret string of characters and is normally the first thing the user provides the system when attempting to "log-on", i.e. to gain access.

For the protection of both the user and the Company, a User ID shall be unique to the user and never shared or known to others, neither during a user's duration with the Company nor thereafter.

No one should be granted a User ID for any Company system unless that person has a recognised need to use the system and has been properly identified and authorised.

Authentication

Before being allowed to log-on to a system and gain access to any resources, the user's identity must be authenticated to prevent impersonation. Whilst passwords will be acceptable on networks, these may not suffice for high risk environments.

Invalid log-on attempts should be considered suspicious and the system should be able to lock out or disable an account after a maximum of 3 invalid attempts. Re-enabling the account should be done manually by DevOps or else in an automated fashion after a delay of at least 15 minutes.

All individual non-console administrative access and all remote access to the systems should be secured using multi-factor authentication.
Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

1. Generic user IDs are disabled or removed;
2. Shared user IDs do not exist for system administration and other critical functions; and
3. Shared and generic user IDs are not used to administer any system components.

Use of these authentication mechanisms (for example, physical or logical security tokens, smart cards, certificates, etc.) must be assigned as follows:

1. Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
2. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

Authorisation
A user or process must be granted the right to access a system. Users with the higher levels of privilege may themselves grant access rights to resources under their control to other users or processes. In all cases, the concept of least privilege or 'need to know' must be adhered to.
Access rights to data files are to be decided strictly on the basis of the content and the role of the user. In particular it is valuable to restrict the use of system administrator, security administrator, database administrator, and similar commands to a limited number of users.

The following steps must be taken before authorisation to access any resource is granted:
1. Establish exactly what resources each person or group of people needs to access and in what way (e.g. READ, WRITE, etc, for files), taking note of anticipated future needs;
2. Standardise user identifiers and task names: the standardised names should preferably reflect the section of the Company for which the data owner works;
3. Define file and other resource naming standards based on the process involved, or the department/unit, or an individual.
IDs used by third parties to access, support, or maintain system components via remote access should be:

- Enabled only during the time period needed and disabled when not in use; and
- Monitored when in use.

4. Termination of User Access
Once an employee's employment is terminated, the System administrator must:

- Notify the respective department and authorise the closing/disabling of the user's account/s; and
- keep all correspondence on file, for reference.

<u>Dormant and dead accounts</u>
Dead or inappropriately privileged accounts should not be left on a system because they could provide the vehicle for misuse. Steps to take should include some or all of these controls:

- removal of vendor's accounts used for setting up the system, or changing their
- passwords as the initial passwords are widely known; and

- introduction of procedures to allow users to request their access rights be revoked for set periods and subsequently restored (to cater for leave, etc);

Unsuccessful login attempts

- The log-on procedure should throw out or lock out a person who has input an incorrect password after a pre-determined number of times;
- The number of attempts permissible before logout should be 3; and
- The user should not be enabled unless properly authenticated. Automatic re-enabling should be after 15 minutes.

5. Compliance

Violation of this policy should be avoided. If deviations are absolutely necessary, then top management authority must be obtained, and documentation kept of the rationale behind the authorisation to deviate.

Employees should report any misuse or abuse of authorisation levels or user accounts or any cases of suspected unauthorised access.

Should an employee have access to resources and is aware that he/she should not have access to such resources, he/she should report it and refrain from using these access rights. Failure to do so will be treated as a violation of this policy.

Password Policy and Standards

1. Ownership

Each user on the system should have a password and that password is the property of that user only. No one else can use that password to access a system. The user is responsible for choosing a password that is difficult to guess and that complies with this security policy.

Administrators and Application Owners should ensure that adequate password controls are supported by applications &/or systems implemented.

2. Password Administration

As each password belongs to the individual user and that password is the key to access the systems, the users, therefore, have a responsibility towards the Company by ensuring that the composition and maintenance of their password conforms to this policy. In this way it will be harder for would-be wrongdoers to compromise the organisation's systems.

The following policy statements are to be applied to all GoBankMe Technologies employees:

1. access policies are based on user roles granting the minimum access required for the job;
2. approvals are to be sought and granted only as required based on the job needs;
3. all users should have their own unique user id;
4. addition, deletion and modification of user ids / credentials should be restricted;
5. GoBankMe Technologies will revoke user ids / credentials of terminated users;
6. vendors, if any require access, should be granted after proper authorisation was previously obtained and documented. Access is to be monitored and disabled when no longer needed;
7. users are to be locked out for a minimum of 30 minutes after 3 failed login attempts;
8. re-authentication or re-activation of the session is required after 10 minutes idle;
9. users are to be disabled if inactive for more than 90 days;

10. two factor methods of authentication is required for remote access;
11. first time passwords must be unique for each user and must be changed following first use;
12. reset passwords must be unique for each user and must be changed following first use;
13. guidance is to be provided to users on how to use strong authentication and strong passwords;
14. passwords are to be changed immediately should any compromise be suspected;
15. group or shared accounts are prohibited;
16. different authentication can be used for each customer; and
17. controls are to be put in place to ensure proper authentication

3.Password Standards

All passwords should meet or exceed the following strong passwords characteristic guidelines.

- Minimum Length of a password must be at least 12 (twelve) characters;
- The password must contain characters from at least three of the following four classes of characters:

Class Examples
English uppercase letters A, B, C
English lowercase letters a, b, c
Westernised Arabic
Numerals 0, 1, 2
Non-alphanumeric (special characters) #, &, !, %, @, ?, -, *

Poor, or weak, passwords have the following characteristics:

- Contain at less than 12 (twelve) characters;
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon;
- Contain personal information such as birth dates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters;
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software;
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321;
- Contain common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret); and
- Are some version of “Welcome123” “Password123” “Changeme123”
- You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "You must remember this password please" could become the password YmRtP18ase! or another variation.

4. Passphrases

Passphrases generally are used for public/private key authentication.
A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access. A passphrase is similar to

a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks.
Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters.

5. Responsibilities and Maintenance

Passwords for systems that interact with the network segment for which the PSI certification is conducted must change every 60 days. The Information Security Officer will send the staff reminders to change passwords. Where in doubt consult the owner/s of the system and data or the Information Security Officer.
Passwords should not be reused until at least 10 (ten) password changes have been carried out. Passwords must not be written down anywhere.
If a password is assigned to you, you must change it immediately to your own personalised password.
Never give your password to anyone or accept a password from anyone, especially over the phone or the Internet.

6. Important Passwords

Every system administrator, firewall administrator, application administrator, back-up administrator, email server and web server administrator possess the Password used to access and administer these systems. The composition of these passwords is of the utmost importance and should be taken very seriously. Without access to this password continuity of operations may be hampered or seriously hindered.

7. Monitoring

Employees of the firm or consultants may, from time to time, be authorised by management to attempt to crack passwords being utilised on our systems by employees. Common cracking tools will be used. Any weak passwords that are discovered will be disclosed only to the employee involved who will also be asked to change it immediately and to avoid using weak passwords.

8. System Security

Preferably, any system in production should be able to automatically enforce the above-mentioned password policies as this will reduce the chances of insecure passwords being used. Therefore, all systems in use that support some or all of the policies in this document should have those features enabled. All efforts should be made to develop or purchase software supporting this policy, where this is cost-effective.
Every system must, as a minimum, contain the following features:

- At no time must a password be displayed in clear text anywhere
- At no time must a password travel over the network in clear text
- At no time must a password be stored in clear text

9. Violation

Since failure to abide by this policy can imperil the Company’s system/s and networks repeated violation of this policy may result in disciplinary action up to and including termination of employment and or legal action if warranted.
Should employees note any misuse of passwords or violations of this policy by their colleagues it should be immediately reported to the Information Security Officer. The names of the persons reporting individuals will be kept confidential at all times.

10. Responsibilities and Maintenance

References

- SANS Consensus Policy Resource Community: Password Construction Guidelines
- SANS Consensus Policy Resource Community: Password Protection Policy

Anti-Virus Policy

The term 'anti-virus software' refers to software which scans and removes malware which includes viruses, Trojans, worms, spyware and adware and protects against all known types of malicious.

All equipment (servers and PCs) should have anti-virus software installed. The only exception to this includes cases where it has been deemed that a specific environment is not vulnerable to viruses and other malware.

For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

Virus definition files should be updated on regular basics.

Anti-virus software should:

- be set to carry out periodic scans;
- be set to run in real-time protection mode;
- be set to send samples of suspicious files to anti-virus vendor for advanced analysis; generate logs which should be retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).
- be actively running and cannot be disabled or altered by users, unless specifically authorised by management on a case-by-case basis for a limited time period.
- Where a PC/server cannot be updated from the internet, the virus definition file should be downloaded to another machine and manually installed on the respective PC/server.
- If the anti-virus software will not be able to clean a virus that was detected, ops must be informed as soon as possible

Monitoring Policy

GoBankMe's Infrastructure monitoring is provided by Railsbank, who are responsible for maintaining the correct time on all components provided.

Log entries are to be generated:

- From all components that store, processes or transmit CHD and/or SAD
- From all components that could impact the security of CHD and/or SAD
- From all critical system components
- From all components that perform security functions

GoBankMe Technologies has implemented automated audit trails for all system components to reconstruct the following events:

- All individual user accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Initialisation, stopping, or pausing of the audit logs

- Creation and deletion of system-level objects

GoBankMe Technologies will record, at a minimum, the following audit trail entries for all system components for each event:

- Date and time
- User ID of user or system component/service generating the event
- Type of event
- Origination of event
- What system component and/data or service was affected
- What the outcome of the event was (success/fail)

Logs are to be retained for a minimum of 1 year with 3 months readily available (online). Review generated logs will be produced, at a minimum, on a daily basis.
Alerts are to be generated as necessary and action taken as per Incident Response Policy. These include, but not limited to:

- Update the risk register:
  o When performing the annual Risk Assessment
  o As needed when new vulnerabilities / risks are encountered

Data Retention and Disposal Policy and Procedures

1. Disposal of Data

Data should be disposed of in accordance to the pre-established retention periods of the respective data type. Past the retention period, data should be adequately destroyed.

Type of Data Retention Period Comments

Credit/debit Card Data:
Up to 6 years but for no longer deemed necessary
Currently PAN, Cardholder Name, Expiration Date is stored. PAN is encrypted
Audit Logs Up to 6 years but for no longer deemed necessary
Visitor Logs Up to 6 years but for no longer deemed necessary

Transactions details:
Up to 6 years but for no longer deemed necessary

Credit/debit Card Data:
1. Maintain an up to date data retention policy, including:
   a. Any legal requirements to retain data
   b. Location where all cardholder data is stored (CDE Matrix)
2. Credit/debit card data should only be retained if there is a valid business requirement for it to be stored.
3. Credit/debit card data which is past the retention period should be removed through an automated process which is carried out at least every quarter. In the event that an automated process is not possible, a manual review has to be conducted at least every quarter to identify data which needs to be deleted.
   a. Enact a quarterly process whereby data that exceeds its retention limit is securely deleted.

4. Apply security policies and operational procedures for restricting access to cardholder data.
5. Retain audit logs, including AV and time, for at least one year with a minimum of 3 months immediately available.
6. Do not retain sensitive authentication data (even if encrypted) (sensitive authentication data: the personal identification number (PIN) or the encrypted PIN block after authorisation, CVV2, CVC2, CID, CAV2 should never be stored, either temporarily or permanently). [unless involved in issuing business]
7. Credit/debit card data printed and stored on paper media (for the duration of the retention period) should always be kept under lock and key.
8. Only users with legitimate business need to see the full PAN. All the others see masked PANs (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.
9. A list of roles that need access to displays of more than the first six/last four (includes full PAN) must be documented, together with a legitimate business need for each role to have such access.
10. Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
    a. One-way hashes based on strong cryptography, (hash must be of the entire PAN).
    b. Truncation (hashing cannot be used to replace the truncated segment of PAN).
    c. Index tokens and pads (pads must be securely stored).
    d. Strong cryptography with associated key-management processes and procedures.
11. Credit/debit card data should be securely deleted from memory after use.
12. Protect keys used to secure cardholder data, as follows:
    a. Maintain a list of personnel entrusted with access to keys
    b. Securely store and limit distribution of keys to those only with a need to know
    c. Retire / replace keys and do not use to encrypt thereafter:
        i. if compromise suspected
        ii. at the end of their crypto period
        iii. when personnel with knowledge of the keys no longer works with the Company
    d. Manual keys, if any, require:
        i. 2 key custodians as a minimum; and
        ii. split knowledge to perform dual control
    e. Maintain a list of where keys are saved
    f. Exchange keys with customers, if required, should be via trusted methods only

2. Disposal of Equipment
If any equipment needs to be removed from the Company's network, the DevOps will ensure that the Hard Disks of such equipment have been completely degaussed. A support ticket needs to be opened with the data centre to ensure this is carried out on behalf of the Company.

Access To and Use of Primary Account Numbers (PANs)
1. Purpose

This policy describes the authorised methods as well as prohibitions in which employees' access and make use of full credit/debit card data. This policy applies, irrespective of the fact that the Company may or may not store credit/debit card data.

2. Scope

This policy applies to all personnel of the Company as well as subcontracted third parties (if such data is made available to them). More specifically, it is intended to employees that have access to PANs for legitimate business reasons.

3. Policy

- Access to the cardholder data is made available only to those individuals with a job function that requires such access. Employees should inform ISO (Information Security Officer) if their access level is not commensurate to their job function.
- Management should ensure that in the interest of security, the list of users with access to cardholder data is kept as small as possible and such list is reviewed and kept updated regularly.
- No cardholder data may be stored in clear text. Storage of card data should be carried out in accordance to the Company's accepted storage methods. No personal storage of such data is allowed and no end-user computing is allowed when dealing with card data.
- All card holder data should be stored in encrypted format using industry accepted encryption algorithms and key management procedures in line with PCI DSS standards.
- Even when in accordance with these secure practices, cardholder data should only be stored if absolutely required.
- If data must be moved on non-encrypted devices or systems (including hardcopies), data must be masked on display and truncated during storage.
- For the avoidance of doubt, truncated credit/debit card numbers a maximum of the first 6 digits and the last 4 digits are not be considered card data and consequently are outside the scope of this policy. Nevertheless, such data should be considered as internal data and not public information.
- Unmasked cardholder data may never be shared through email, sms or any other messaging technology.
- Storage, even temporarily, of CVV data is strictly forbidden.

4. Compliance

Managers are responsible for reviewing this and other policies with their employees, and monitoring compliance with these policies.

Employees in violation of these policies are subject to possible disciplinary action including dismissal.

Data Ownership and Classification Policy

1. Purpose

Data is one of the Company's most valuable assets and requires responsible and ethical use. It is essential that the Company's data is classified so that security measures can be correctly implemented. It is also necessary to assign responsibilities to the handling of all data held so that security measures may be implemented and monitored.

2. Responsibilities

Data owners

Owners are responsible for knowing, understanding and classifying all data they own. They are also responsible for ensuring that adequate security is applied to the data in accordance with the classification assigned by them and that the security satisfies all legal requirements.

Only they may authorise persons to access the data and they decide the access rights to be assigned.

Data custodians/processors

Custodians are responsible for data entrusted to them for periods of time irrespective of the format. They are responsible for ensuring that the level of security required to protect the data is maintained during their custodianship. Examples of custodians would be DevOps.

Data users

Users have been granted access rights to the data by the owners so that they may carry out their duties and responsibilities. Users may not abuse of the rights given to them and may only do that which they have been authorised to do by the owners.

Management

The owners of data and the custodians are to be appointed by management after an understanding of the data and the roles of individuals have been achieved.

3. Assigning Ownership

The overall ownership of the data rests with the Company. However, the responsibility and authority over that data will be delegated to the required Company departments as deemed necessary. In doing so, however, it is recognised that ownership responsibility is not a single all-or-nothing dictatorial concept; but rather it is comprised of a set of responsibilities.

4. Data Classification Standards

This policy outlines the extent to which the data classification standard should be followed, the responsibilities of the departments' employees to the standard, and provides guidelines for classifying the data.

Five levels of data classification have been established.

1. Unclassified/Public Domain - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific Data Owner approval;
2. Operational Use Only - data whose loss, corruption or unauthorised disclosure would not necessarily result in any business, financial or legal loss, but is made available to Data Owner approved users only;
3. Private - data whose disclosure would not result in any business, financial or legal loss but involves issues of personal credibility, reputation, or other issues of personal privacy;
4. Confidential - data whose loss, corruption or unauthorised disclosure would tend to damage the business, image, reputation or research capabilities of the Company, or result in business, financial, or legal loss;
5. Top Secret - data whose loss, corruption or unauthorised disclosure would be a violation of laws and regulations.

All data regardless of medium and/or form will be identified as to its classification (i.e. Unclassified, Operational Use Only, Private, Restricted or Confidential).

Aggregates of data should be classified based upon the most secure classification level; in other words, when data of mixed classification exist in the same file, report or

memorandum, the classification of the same file, report or memorandum should be of the highest level of classification.

5. Data Protection Measures

Public Domain data requires no specific protection either during storage or transmission.

The availability and integrity of Operational Data must be protected during transmission and storage. Systems housing and carrying such data must be securely configured and message authentication utilised during transmission. Adequate back-up of such data must be regularly taken and stored both on-site and off-site.

Private Data must be afforded the same level of control as operational data. In addition, should such data travel over a public network, it must do so in encrypted format to preserve confidentiality.

Access to confidential data must at all times be strictly on a need to know/least privilege basis.

Such data must always be transmitted in encrypted format.

Top Secret data must be afforded the highest levels of control at all times. Encryption during storage and transmission using the strongest techniques available. Furthermore, networks or databases housing such information should be segregated from other networks.

Outsourced Services

The Company has to continually track the purpose, scope and compliance status of the services it outsources from service providers. The full list of services should be documented in the lists below together with whether the service is relevant and in scope of PCI DSS. In the event that the particular service provided addresses a requirement in PCI DSS, the requirement reference number is to be indicated and a confirmation that the service is either PCI DSS compliant or alternatively the service provider being in possession of PCI DSS Certification.

All third-party companies providing critical services (Cardholder data interchange) to GoBankMe Technologies must provide an agreed Service Level Agreement (SLA).

All third-party companies which have access to Card Holder information must

1. Adhere to the PCI DSS security requirements;
2. Acknowledge their responsibility for securing the Card Holder data;
3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law;
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure;
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party; and
6. Acknowledge that these agree obligations to safeguard the confidentiality of the CardHolder data shall survive the termination of any other contractual agreements with GoBankMe.

Where the third-party is providing an outsourced software development service, the following issues should be addressed before any contractual arrangements or agreements are

entered into:

1. Licensing agreements, code ownership and intellectual property rights;
2. Certification of the quality and accuracy of work carried out;
3. Rights of access to audit the quality and accuracy of work done or in progress;
4. Contractual requirements for quality of code; and
5. Full review of source code and testing before installation to attempt to detect Trojan Code.

Where a software exchange or data exchange is to take place with the third-party the security content of all agreements, legally binding or other, must considers the following points:

1. Responsibilities for controlling and notifying transmission, dispatch and receipt;
2. Minimum technical standards and protocols for packaging, transmission and decoding;
3. Responsibilities and liabilities in the event of loss of data;
4. Information and software ownership with attendant legal responsibilities, e.g. data
5. protection; and
6. Special controls, e.g. cryptographic keys

Where contractual agreements are already in places which do not have the above controls in place, the controls and clauses must be added to the contract as a precursor to any renewal.

1. Enforcement

Any violation of standards, procedures or guidelines established pursuant to this policy shall be presented to the management of the organisation for appropriate action. This could result in disciplinary action, including dismissal or discontinuation of service and/or legal prosecution.

Information Security Awareness Program

The Company must regularly inform all users about information security requirements and allocate resources to build and maintain a security awareness program. The purpose of a security awareness program is to explain to personnel the importance of the information they handle and the legal and business reasons for maintaining its confidentiality. Employees must understand their responsibilities and the steps the organisation will take to ensure security

A security awareness program is tailored to the Company. It should focus primarily on security issues common to most or all employees. A security awareness program should cover:

1. What information should be protected
2. Security measures employees can take
3. What employees should do if a problem is found

Program

The Program consists following actions:

1. Determine employee's roles (see 'Roles' item)

2. Provide lists of documents to read and sign in “security awareness” journal for each role (see ‘Documents’ item)

Roles

Role1 - Company’s employees who have access to cardholder data (CHD)

Role2 - Company’s employees who do not have access to CHD

Documents

Roles 1:

1. Cardholders Data Retention Policy (part of Information Security Policy)
2. Password Policy
3. Access Policy to Cardholders Data (part of Information Security Policy)
4. Media Usage Policy (part of Information Security Policies)
5. Physical Security Policy CDE

Roles 2:

1. Password Policy
2. Physical Security Policy CDE

File Integrity Monitoring Policy

A file-integrity monitoring tool is deployed to alert personnel of unauthorised modification of critical system files, configuration files, or content files.

File integrity checking is performed automatically by the software package OSSEC.

OSSEC classifies all changes in configurations in three categories:

1. Low Importance
2. Medium Importance
3. High Importance

OSSEC sends information about these changes to dedicated personnel in Security & Risk Department.

A Risk Manager will perform daily reviews of logs generated according to following steps:

1. Analyses logs

2. Compares to the Dictionary of Non - Critical type of Events. If the Event is not listed in the Pre-defined list of non-Critical type of events then the:

- Event is marked as Critical for further analyses
- After the review, the Risk Manager sends the notification about the detected changes to System Administrators Unit and asks them to give a feedback on the changes for the clear analysis.
- At the End of the Working Day, a Gathered Information Report is sent to the Chief Security Officer & back-end development team lead for Further in-Depth Analyses.
- The Technical board makes decisions and re-classifies events reported in the weekly package:
    1. Non-Critical
    2. Critical - Requires Further Investigation o Critical events are reported to CEO.
    3. Critical – Requires Actions.
       A Change Request is formulated by Security Officer and registered in IT.

Key Management Policy

1. Card Holder Data Encryption

Generation

For storing cardholder data.

For data encryption we use Transparent Data Encryption. Transparent Data Encryption (TDE).

Storage

TDE encrypts the storage of an entire database by using a symmetric key called the database encryption key (DEK). This database encryption key is protected by the TDE protector, which is either a service-managed certificate ("Service-Managed TDE"). The TDE protector is set at the server level.

Usage

On database start-up, the encrypted DEK is decrypted, and then used for decryption and re-encryption of the database files in the SQL Engine process. TDE performs real-time I/O encryption and decryption of the data at the page level. Each page is decrypted when read into memory and encrypted before being written to disk.

2. Token Key

The default setting for TDE is that the database encryption key is protected by a built-in server certificate. The built-in server certificate is unique for each server. If a database will be in a geo-replication relationship, both the primary and geo-secondary database will be protected by the primary's parent server key.

Bring Your Own Key (BYOK) support allows the user to take control over their TDE encryption keys and control who can access them and when. With BYOK, the database encryption key is protected by an asymmetric key stored in AKV. The asymmetric key never leaves Key Vault; once the server has permissions to a key vault, the server sends basic key operation requests to it through the Key Vault service. The asymmetric key is set at the server level and inherited by all databases under that server. With BYOK support, users can now control key management tasks including key rotations, key vault permissions, deleting keys, and enable auditing/reporting on all encryption keys. Key Vault provides central key management, leverages tightly monitored hardware security modules (HSMs).

Patch Management Policy

This document describes the handling, responsibilities and scope of Patches, configuration Updates and system Upgrades managed in the Company. The document is currently effective throughout the Company and applies to all employees and software systems. The misuse or violation of any instruction or procedure mentioned in given document is subject of report to the top management of the Company.

1. Definitions, main characteristics & categories
    1. Patch levels are application, DB, configurations.
    2. Patches and fixes of database systems are conducted by database administrator (DevOps and back-end development team lead).
    3. Administrators duties cover tracking of new patches or update issuances.

4. All Principal solutions for Payment system are fully provided by inside software development division. Any updates, upgrades and changes in software platform, its separate modules or functions are supplied by inside software development division.
5. All vulnerabilities found during internal, external (AWS, penetration) scanning process must be delivered to corresponding employees and fixed with same procedure described in this document below.

2. Policy

Patches/Fixes/Upgrades of all systems are subject to the following rules:

1. Any system update must be tested in test machine or environment before deploying on production.
2. Conclusion of successful testing should exist for any update on product system
3. All updates or bug fixes on any system in the Company are to be stored and tracked in SPECIAL JOURNAL (Jira)
4. Any update or fix on production system should be approved by TOP Management.
5. Permissions for updates on production systems should be limited only to designated personnel which is appointed by executive management of the Company
6. A configuration and data backup should be performed before each update/upgrade of production system

3. Procedure Description

All updates and fixes performed on payment system are implemented only with existence of patch itself, installation manual, descriptions of changes and description of how it affects system functionality, list of target systems, receipt date of updates, testing results & approving for implementation on production system.

All this information is tracked in according change request form. If any of the required components is missing, update should not be performed unless there is an approval of top management of the Company.

Update process is logged and journalised.

Physical Security Policy

Servers Physical Security

Workstations physical security

1. Access to the Company’s office with listed in CDE Matrix staff is restricted and may be possible only using personal passes
2. Access to office is fixed by video cams
3. To access the Company’s office, a visit log is kept
4. Office building is on all-day surveillance by security

Data transfer

All data is transferred via channels in encrypted form. When data is transferred on physical media, the data must also be encrypted

Backups

1. Backup media should be stored in closed safes or rooms
2. Regular backup copies (at least once a month) should be stored outside the Company's office
3. Backup copies should be transported with precautionary measures (as well as when transporting valuables)

Hard disks

1. Removable hard drives should only be used in case of emergency
2. Avoid copying data to removable media
3. From removable media should be discarded except when the local network is extremely unprotected. Removable disks can be more secure than the server, since the data is stored locally. In this case, the discs must be stored in closed safes
4. Confidential data must be encrypted. If the server on the network is considered unreliable, the files can be processed locally, encrypted and then stored on the server. This is preferable to using removable disks, as server data is regularly backed up. The risk of data loss is minimised (except when the encryption key is lost or forgotten)
5. Prevent the repair of confidential disks, they must be destroyed

Printers

Card data or any confidential information must not be recorded, stored or printed in paper format in the Company's offices

Computers/notebooks

1. Must be set passwords for BIOS on work stations of listed in CDE Matrix staff
2. When downtime is more than 5 minutes, the screens should automatically shut down and be blocked with a password
3. Computer enclosures should be closed as far as possible

<u>NTP Synchronisation Schema and Procedure</u>

1. Purpose

This procedure sets out the principles to address the acceptability of architecture and configuration of NTP within organisation’s critical IT infrastructure.

2. Scope

In all critical systems time synchronisation technology must be implemented to ensure that systems have the correct and consistent time and time settings are received from industry-accepted time sources.

3. Procedure

NTP Synchronisation Schema meets following PCI DSS requirements:

1. Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic
2. Time or UTC (time settings are received from industry-accepted time sources).
3. Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.
4. Systems receive time only from designated central time server(s).
5. Time data is protected (access to time data is restricted to only personnel with a business need to access time data, any changes to time settings on critical systems are logged, monitored, and reviewed).