Information Technology Policy

GTP FINANCE LIMITED

Contents

Introduction

The GTP Finance IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the company which must be followed by all employees. It also provides guidelines GTP Finance will use to administer these policies, with the correct procedure to follow.

GTP Finance will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcomeand will be examined for improvements within the regulatory framework.

These policies and procedures apply to all employees, contractors, consultants, temporaries, and other workers at GTP Finance, including all affiliates.

Acceptable Usage Policy

Overview

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, voice and mobile IT equipment, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of GTP Finance. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every GTP Finance employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at GTP Finance. These rules are in place to protect the employee and GTP Finance. Inappropriate use exposes GTP Finance to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GTP Finance business or interact with internal networks and business systems, whether owned or leased by GTP Finance, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at GTP Finance and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with GTP Finance policies and standards, and local laws and regulation.

This policy applies to all employees, contractors, consultants, temporaries, and other workers at GTP Finance, including all personnel affiliated with third parties (hereafter referred to as ‘Individuals’). This policy applies to all equipment that is owned or leased by GTP Finance.

Policy

1.1 General Use and Ownership

1.1.1 GTP Finance proprietary information stored on electronic and computing devices whether owned or leased by GTP Finance, the employee or a third party, remains the sole property of GTP Finance. It mustbe ensured through legal or technical means that proprietary information is protected.

1.1.2 Individualshave a responsibility to promptly report the theft, loss or unauthorized disclosure of
GTP Finance proprietary information.

1.1.3 Individuals may access, use or share GTP Finance proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

1.1.4 For security and network maintenance purposes, authorized individuals withinGTP Finance may monitor equipment, systems and network traffic at any time.

1.1.5 GTP Finance reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.2 Security and Proprietary Information

1.2.1 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
1.2.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less.Individualsmust lock the screen or log off when the service is unattended.
1.2.3 Postings by individualsfrom a GTP Finance email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of GTP Finance, unless posting is in the course of business duties.
1.2.4Individualsmust use extreme caution when opening e-mail attachments received fromunknown senders, which may contain malware.

1.3 Unacceptable Use

The following activities are, in general, prohibited. Individualsmay 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 is an individualof GTP Finance authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing GTP Finance-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.

1.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company 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 GTP Finance.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which GTP Finance or the end user does not have an active license is strictly prohibited.
3. Accessing data, server or an account for any purpose other than conducting GTP Finance business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing account password to others or allowing use of account by others. This includes family and other household members when work is being done at home.
7. Leave their user accounts logged in at an unattended and unlocked computer.
8. Use someone else’s user ID and password to access GTP Finance IT systems.
9. Leave their password unprotected (for example writing it down).
10. Perform any unauthorized changes to GTP Finance IT systems or information. Attempt to access data that they are not authorized to use or access.
11. Exceed the limits of their authorization or specific business need to interrogate the system or data.
12. Connect any non-GTP Financeauthorized device to the GTP Finance network or IT systems.
13. Store GTP Finance data on any non-authorizedGTP Finance equipment.
14. Give or transfer GTP Finance data or software to any person or organizationGTP Finance without the authority of GTP Finance.

15. Using a GTP Finance computing asset 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.

16. Making fraudulent offers of products, items, or services originating from any GTP Finance account.

17. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

18. 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 authorized 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, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

19. Port scanning or security scanning is expressly prohibited unless prior approval to GTP Finance Director - Technology is made.

20. 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.

21. Circumventing user authentication or security of any host, network or account.

22. Introducing honeypots, honeynets, or similar technology on the GTP Financenetwork.

23. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

24. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

25. Providing information about, or lists of, GTP Finance employees to parties outsideGTP Finance.

1.3.2 Internet, Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are their own and not necessarily those of the company".

Individuals must not:

1. Use the internet or email for the purposes of harassment or abuse. Use profanity, obscenities, or derogatory remarks in communications.
2. Access, download, send or receive any data (including images), which GTP Finance considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.

3. Use the internet or email to make personal gains or conduct a personal business. Use the internet or email to gamble.
4. Use the email systems in a way that could affect its reliability or effectiveness, forexample distributing chain letters or spam.
5. Place any information on the Internet that relates to GTP Finance, alter any information about it, or express any opinion about GTP Finance, unless they are specifically authorized to do this.
6. Send unprotected sensitive or confidential information externally.
7. Forward GTP Finance mail to personal non-GTP Finance email accounts(for example a personal gmail account).
8. Make official commitments through the internet or email on behalf of GTP Finance unless authorized to do so.
9. Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
10. In any way infringe any copyright, database rights, trademarks or other intellectual property.
11. Download any software from the internet without prior approval of the IT Department.
12. Connect GTP Finance devices to the internet using non-standard connections.

1.3.3 Blogging and Social Media

1. Blogging by individuals, whether using GTP Finance'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 GTP Finance's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate GTP Finance's policy, is not detrimental to GTP Finance's best interests, and does not interfere with an employee's regular work duties. Blogging from GTP Finance's systems is also subject to monitoring.

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

3. Individuals shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of GTP Finance and/or any of its employees. Individuals are also prohibited from making any discriminatory, disparaging, defamatory or harassingcomments when blogging or otherwise engaging in any conduct prohibited by GTP Finance.

4. Individuals may also not attribute personal statements, opinions or beliefs to GTP Finance when engaged in blogging. If an individual 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 GTP Finance. Individuals assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, GTP Finance's trademarks, logos and any otherGTP Finance intellectual property may also not be used in connection with any blogging activity

6. Accessing any social media website including but not limited to facebook, twitter, youtube, instagram are prohibitedin GTP Finance owned systems and prohibited inside GTP Finance premises.

1.3.4Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, GTP Finance enforces a clear desk and screen policy as follows:

1. Personal or confidential business information must be protected using security features provided for example secure print on printers.
2. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
3. Care must be taken to not leave confidential material on printers or photocopiers.
4. All business-related printed matter must be disposed of using confidential waste bins or shredders.

1.3.5Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

1. Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
2. Laptops must be carried as hand luggage when travelling.
3. Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
4. Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

1.3.6Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of

transferring data. Only GTP Financeauthorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

1.3.7Software

Employees must use only software that is authorized by GTP Finance on GTP Finance computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on GTP Finance computers must be approved and installed by the GTP Finance IT department.

Individuals must not:

Store personal files such as music, video, photographs or games on GTP Finance IT equipment.

1.3.8Viruses

All PCs have antivirus software installed to detect and remove any virus automatically. The IT Administrator will maintain all antivirus software.

Individuals must not:

1. Remove or disable anti-virus software.
2. Attempt to remove virus-infected files or clean up an infection, other than by the use of approved GTP Finance anti-virus software and procedures.

1.3.9Telephony (Voice) Equipment Conditions of Use

Use of GTP Finance voice equipment is intended for business use. Individuals must not use GTP Finance voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual’s own expense using alternative means of communications.

Individuals must not:

1. Use GTP Finance voice for conducting private business. Make hoax or threatening calls to internal or external destinations.
2. Accept reverse charge calls from domestic or International operators, unless it is for business use.

1.4 Actions upon Termination of Contract

All GTP Finance equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to GTP Finance at termination of contract.

All GTP Finance data or intellectual property developed or gained during the period of employment remains the property of GTP Finance and must not be retained beyond termination or reused for any other purpose.

Policy Compliance

1.1 Compliance Measurement

The GTP Finance will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits.

All data that is created and stored on GTP Finance computers is the property of GTP Finance and there is no official provision for individual data privacy, however wherever possible GTP Finance will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. GTP Finance has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

It is the responsibility of everyemployee responsibility to report suspected breaches of security policy without delay to your line management, or the IT department.

1.2 Exceptions

Any exception to the policy must be approved by the GTP Finance Director - Technology in advance.

1.3 Non-Compliance

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Core banking software policy

Introduction

The company in accordance to the decision of the board will outsource software for its day to day operations. The shortlisting and finalizing the software, its terms of service , commercials will be approved internally by a committee headed by the Director (technology) and such approvals will be reported to the Managing Director for noting. All such outsourcing will be within the guidelines prescribed by Reserve Bank of India in its Master Direction DNBS.PPD.No.04/66.15.001/2016-17 June 08 2017.

GTP Finance's currentcore banking software is "Shakti"software provided by QbrikGTP Finance uses the software in SAAS (Software as a Service) model. Shakti is a web application which has various modules: (1) Customer management, (2) Loan management, (3) Deposit management, (4) Daily Branch Operations, (5) Admin module, (6) Finance & HR module, and (7) Reports module.

Below are the guidelines set forward to maintain the security and integrity of the information captured and stored in the software and to avoid any malpractices.

Policy

User Access Control

Each employee will be given access to the different operations in Shakti based on their designation. Access to the data will be given based on the branch they belong. A role-based access control is implemented in Shakti. Following is the role-based access that should be set in Shakti.

Designation	Division	Role access in Shakthi	Branch Access in Shakthi
Director - Operations	Head Office	APPROVE HIGH VALUE LOANS, VIEW REPORTS	All branches
Project Co-ordinator	Head Office	APPROVE HIGH VALUE LOANS, VIEW REPORTS	All branches
Director - Technology	Head Office	Admin (Super Admin)	All branches
Accountant	Head Office	GL ACCOUNTANT, AF ACCOUNTANT, ACCOUNTING ADMIN	All branches
Administrator	Head Office	AF BRANCH OPS, AF PAYMENT, AF DEPOSIT, VIEW REPORTS, AF EOD, CONFIRM EOD COMPLETION	All branches
IT Administrator	Head Office	IT ADMIN	All branches

Credit Manager	Head Office	AF CUSTOMER ENROLMENT, AF LOAN ORIGINATION, AF REVIEW, AF VEHICLE MASTER, AF CREDIT APPRAISAL, AF VIEW REPORTS	Asset Finance Division branches
Assistant credit manager	Head Office	AF CUSTOMER ENROLMENT, AF LOAN ORIGINATION, AF REVIEW, AF VEHICLE MASTER,AF VIEW REPORTS	Asset Finance Division branches
Manager	Asset Finance	AF CUSTOMER ENROLMENT, AF LOAN ORIGINATION, AF REVIEW, AF VIEW REPORTS	Branch-level access
Back-office executive	Asset Finance	AF CUSTOMER ENROLMENT, AF LOAN ORIGINATION, AF VIEW REPORTS	Branch-level access
Administrator	Gold Division	GL ADMIN	Gold Division branches
Assistant Administrator	Gold Division	GL ASST ADMIN	Gold Division branches
Area Manager	Gold Division	GL AREA MANAGER	Group of branches
Branch Manager	Gold Division	GL BRANCH MANAGER	Branch-level access
Assistant Branch Manager	Gold Division	GL ASST BRANCH MANAGER L1/L2	Branch-level access
Business Executive	Gold Division	GL BUSINESS EXECUTIVE	Branch-level access

In head office and asset division, to change access for a user an approval should be first received from Director – Operations, Director – Technology. Once approved, the IT administrator should make the change in the application. In gold division, to change access for a useran approval should be first received from Project coordinator/ Consultant and Director-Technology. Laterthe gold division administrator should make the change in Shakti.

Loan Approval Slabs

Approval slabs are implemented in Shakti application. Based on employee title the approval slabs are to be fixed. Any change in approval slabs requires an approval from the Director – Operations. Once approved, the change is applied in Shakthi by Super Admin user.

Loan approval in gold division will be done in the branch level by assistant branch manager or branch manager based on their approval slabs. In asset finance division, loan approval will be done by credit manager.

In gold division, all high value loans above INR 10 lakhs are to be approved by Project Coordinator or Director – Operations. The powers so delegated will be in accordance to the Board approved loan Policy.

Maker Checker

All loan products origination and approval process in Shakti will follow the maker checkervalidation. Maker checker validation is implemented in Shakti application. So, the same user cannot originate and approve the loan.

Reports

A reports module is implemented in Shakti application which enables to draw various reports needed for the management purpose and also reports needed for RBI regulation. All accounting reports, collection reports, interest income reports can be readily accessed from shakti application. The report module has a feature called Accounts Qbe which has the flexibility to draw different reports in real time based on the criteria's given by the user. The various reports module present in Shakti application are as below:

1. Accounting reports
2. Operational reports
3. Static reports
4. Exception reports
5. PAR reports
6. Future cash flow reports
7. Account Qbe

Password policy

Introduction:

- Password are an important aspects of computer security. All staff including branch staff with access to company name system are responsible to select and secure password. The purpose of this policy is to establish a standard for creation of strong password and the protection of those password.
- Password policy is applicable for all client system, core banking application, email application by the company.

Policy

Password Protection

- All user level and system level password must conform to the password guidelines.
- User must use a separate unique password for each of their work-related accounts.
- User may not use any work-related passwords for their own, Personal accounts.
- Passwords must not be shared with anyone, including employee and co-employee. All passwords are to be treated as sensitive, confidential.
- Passwords must not be shared over the phone to anyone.
- Not to write down the passwords
- Ensure loggingout of accounts at the end of day
- Not tosave password in the browsers
- Never give out password in phone calls or emails
- Do not login to the account in Public computers if it looks suspicious

Reset Password

- The local administrator password should be reset every 90 days for greater security and the service account password should be reset at least once in six months.In Shakti software there will give a warning pop up one week ahead of the expiry of the password period suggesting change of password.

Minimum Password Length

- The minimum length of Password for the organizationusers will be preset in the parameter. Once the minimum length is set, next time the users change their Passwords, they will be forced to choose password with minimum characters chosen in the Policy. As per the company policy minimum length required for passwords is 8character's

Mixed Password

- The core banking application and zoho mail has mixed password criteria to make the password stronger. The user needs to have at least one upper case alphabet (A to Z) and one lower case alphabet (a to z) and one special characters (&,#,@...) in the password.

Password Audit policy

- Inzoho mailthe Password Audit policy should be enabled which allows to track all password changes. By monitoring the modifications that are made it is easier to track potential security problems using admin activity report.

Account Lockout

- In the core banking application in order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all users.
- Accounts will lockout after Five (5) invalid password attempts.
- It will be unlocked by administrator with team leader approval.

E-Mail Notifications

- Inzoho mail create e-mail notifications prior to password expiry to remind your users when it's time to change their passwords before they actually expire.

IT Disaster Recovery Plan

Introduction

This section covers the process and disaster recovery procedures in place at GTP FINANCE LTD(GTP) in case of a disaster. The disaster can be a geographical disaster or any other failure that leads to the critical application downtime. The purpose of this section is to ensure minimal downtime, data integrity and availability, in case of a disaster. This section will try to cover all the aspects that should be taken care in case of a disaster. This document outlines the process and procedures that will help us overcome the disaster with minimal effect on the working of our organization.

Critical Application assessment

GTP's critical application is our core banking software (CBS) from the vendor Qbrik. Qbrik provides CBS in Software as Service (SaaS) model. The server and GTP's finance system database is maintained by Qbrik. CBS is the critical application as any failure of it will nearly halt our operations in all branches especially the gold loan division branches. But as per SLA with Qbrik, procedures are in place for the CBS application to be up within a span of 4 hours.

CBS Application Server Location (provided by Qbrik)

1. Primary Server: AWS India
2. Secondary Server: AWS India

Database Backup Procedures

1. Qbrik's Database Backup Procedure

   Qbrik takes daily evening database backup before the EOD process is started and after completion of the EOD process.
   EOD : End of Day

2. GTP's Database Backup Procedure

a. Encrypted Database backup
Qbrik provides daily encrypted database backup to GTP's Amazon AWS S3 storage. From there GTP takes a daily backup of the recent encrypted database in S3 to its secondary storage device located in Chennai. In S3 storage, GTP maintains only the latest encrypted database backup.

b. Readable Data Backup
Qbrik provides daily readable format backup to GTP's Amazon AWS S3 storage. From there GTP takes a daily back up to a secondary storage device located in Chennai. Every 6 months the readable format backup is removed from S3 storage.

Emergency Key Personnel ContactInfo

Emergency SituationSpokesperson

Name: Divya. M
Division: IT Support
Mobile Number: +91 9790964671
Email: divya.m@gtpfinance.com

The list of key personnel shown below are the employees who are in the respective rolls. Currently the Director (Technology) will be the authority to change / modify the list as and when required. Such modifications will be published as and when necessitated.

CBS Application Support Team

Category	Name	ContactOption	ContactNumber
IT Administrator	Sowthri	Work	+91 44 28295783
		Mobile	91 9500167215
		Email	itadmin@gtpfinance.com
Gold Loan Division Contact	Subha Keerthi	Work	+91 427 2449337
		Mobile	+91 9787507639
		Email	Info.gold@gtpfinance.com
	Deepa	Work	+91 427 2449337
		EmailAddress	Info.gold@gtpfinance.com
Asset Finance Division Contact	Aravinth	Work	+91 427 2449337
		Mobile	+91 9994786093
		EmailAddress	info@gtpfinance.com
	Prasath	Work	+91 427 2449337
		Mobile	+91 9994786093
		EmailAddress	credit@gtpfinance.com

External Vendor: QBRIK Contact	Bhaskar	Work	+91 44 42555570
		Mobile	+91 9884437340
		Email Address	bhaskar@qbrik.in
	Nandhini	Work	+91 44 42555570
		Mobile	+91 8220693192
		Email Address	nandhini@qbrik.in
	Qbrik Support	Work	+91 44 42555570
		EmailAddress	support@qbrik.in

Disaster Assessment

Following are the potential disruptive threats which can occur at any time and affect the normal business process. The results of our deliberations are included in this section. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential Disasters have been assessed as follows	**Probability Rating**	**Impact Rating**	**Remedial Actions**
Non-availability of CBS application	2	3	GTP follows the incident management process for non-availability of CBS application.
Loss of communication network services in the branch level	1	4	1 ISP vendor Dongle present in case the primary internet connection is not working

Probability: 1 = Very High, 5 = Very Low
Impact: 1 = Total destruction, 5 = Minor annoyance

Non-availability of CBS application - Incident Management Process

1. Emergency service people should be contacted at GTP and Qbrik
2. Key persons informed
3. Branch-level staff will take up the manual process until the application is up.
4. Qbrik provides regular updates to GTP
5. Qbrik works on bringing the application up and running.
6. Once CBS is up Qbrik informs GTP
7. The branch level staff updates data captured to the system
8. Qbrik monitors the application performance until EOD.

The IT Policy duly approved by the Board will be circulated among the Operating staff.