LT Group, Inc.

LTG Access Control Policy

Table of Contents

1 OBJECTIVE

The regulations for access control and control of privileges for each one of the users and groups must be clearly specified within LT Group, Inc. (LTG)'s access control policy with the aim of protecting the assets and business processes associated with these assets.

2 SCOPE

This document is applicable to all the resources that requires configuration of user privileges. Below resources are identified to be covered by this policy:

a. Active Directory Accesses
b. Email Accounts (Access for Troubleshooting purposes)
c. Online Systems
d. Client-to-Server Accesses
e. Door Accesses
f. Partner Systems (Access to Technology / Product Customer site)
g. Shared Folders (One Drive and SharePoint)
h. System applications (Access for Build, Testing and Troubleshooting purposes)
i. Project Specific Servers (Access for Build, Testing and Troubleshooting proposes)

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG Information Classification Policy
LTG Policy for the Use of Assets

4 POLICY STATEMENT

4.1 Access Control Policy

Access control and control of privileges to all users of the information systems and physical accesses will be managed and controlled in accordance with the following compulsory directives:

- Access requirements will be established individually for each one of the applications.
- All the information related to the applications will be identified in conjunction with the associated risks.
- Policies and procedures will be established to distribute and authorize access to information.
- The consistency between access control and classification of the information about the different networks and systems must be verified.
- Applicable legislation and any other contractual obligations that affect protection of access to information must be taken into account.
- New access requests shall undergo an approval process.
- Profiles will be created in accordance with the functions to be performed.
- Access Right Management will be undertaken for all environments.
- The access roles will be separated in accordance with the activities to be performed.
- Changes to existing accesses shall be reviewed and approved.

- Procedures for applying for authorizations for access to the systems and applications within the scope of the Information Security Management System will be established.
- Access authorization controls and the removal of access rights will be periodically reviewed.

4.2 Review of the Access Control Privilege

The Access Control privilege will be reviewed and maintained by System Owners, Project Managers or Administrators of the specific applications, folders and servers.

Compliance audit of accesses to application systems, folders and servers shall be performed at least once a month by the IT Infra Security.

5 GUIDELINES

- Any request for access to certain information system and physical access to any working environment within LTG offices shall undergo proper request procedures and approval from an authorized person.
- Removal of user accesses, especially for those leaving the company, must be immediately requested to the proper owners of the systems or to the LTG IT Infra at ltginfra@ltg.com.ph

6 RESPONSIBILITY

Process	R Responsible	A Accountable	C Consulted	I Informed
Identification and request for access rights for each employee and which systems will be accessed	Project Manager / Department Head	Department Head	HR/IT Infra / Administrative Services	Information Security Office
Definition, Review and Maintenance of the access control privileges	System Owners, Administrators (System and Application) and Project Managers	Department Head	IT Department	Information Security Management System Team
Request for removal of user access for separated employees	HR	HR Head	Project Managers/Department Head	IT Infra/Administrative Services/ Information Security Office

Removal of user access for separated employees	IT Infra / Administrative Services	IT Head	HR / Information Security Office	Project Managers / Department Head

7 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or

- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT GROUP, INC.

LT Group, Inc.

LTG E-Mail and Collaborative Tools Policy

Table of Contents

1 OBJECTIVE

To ensure the proper usage of LT Group, Inc. (LTG or the Company) e-mail facility, other collaborative tools (i.e. Microsoft Teams and other tools) and to prevent the negative impacts of its misuse upon employee productivity and reputation of the business.

2 SCOPE

This policy applies to all employees of LTG with access to the corporate email and collaborative related tools.

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System

4 POLICY STATEMENT

4.1 General Use of E-Mail

All employees of LTG are permitted and encouraged to use the LTG e-mail facility, where such use supports the goals and objectives of the business. However, all employees shall ensure that they:

- Comply with the policies defined in this document
- Use e-mail in an acceptable way
- Do not create unnecessary business risk to the Company by their misuse of the email facility

Employees shall use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.
All e-mail correspondences shall be appropriately protected and shall comply with the related information security policies in place.
The corporate e-mail shall not be used to reveal any confidential information of the Company to third parties, except when carried out for strictly professional purposes and with prior consent of LTG.

4.2 Inappropriate use of E-Mail

The following are strictly prohibited:

- Introducing any form of computer virus or malware into the corporate network
- Using company communications systems to set up personal businesses or send chain letters
- Forwarding company confidential messages to external locations
- Viewing, distributing, disseminating, or storing images, texts, or materials that might be considered indecent, pornographic, obscene, or illegal
- Viewing, distributing, disseminating, or storing images, texts, or materials via e-mail that might be considered discriminatory, offensive, or abusive in that the context is a

personal attack, sexist, or racist, or might be considered harassment
- Distributing or using copyrighted information without the proper authorization
- Breaking into the Company's or another organization's system through e-mail
- Using another employee's password/mailbox without proper authorization
- Broadcasting unsolicited personal views on social, political, religious, or other non-business-related matters
- Transmitting unsolicited commercial or advertising materials
- Undertaking deliberate activities that waste staff effort or network resources

4.3 Personal Use

Employees are allowed to use their corporate email for some personal reasons. For example, employees can use their corporate email to:

- Register for classes or meetups.
- Send emails to friends and family as long as they don't spam or disclose confidential information.
- Download ebooks, guides and other content for their personal use as long as it is safe and appropriate.

Employees must adhere to this policy at all times, in addition to our confidentiality and data protection guidelines.

4.4 Email security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.
Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every two months.

Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can ask our [LTG IT]
We remind our employees to keep their anti-malware programs updated.

4.5 Monitoring and Inspection

- All employees shall keep in mind that the LTG owns any communication sent via the LTG e-mail facility or stored in company devices.
- Employees shall never consider electronic communication, storage, or access to be private, if it is created or stored in company devices.
- Management and other authorized staff have the right to inspect, monitor, or cancel access to private mailbox under any of the following circumstances:

  - ✓ Legal requirements
  - ✓ Confirmed suspicion of a violation of the Company's internal policies, such as engaging in electronic commerce, falsification of addresses, etc.
  - ✓ Emergency situations in which not acting could seriously affect the Company's general service.

4.6 E-mail signature

We encourage employees to create an email signature that exudes professionalism and represents our company well. Salespeople and executives, who represent our company to customers and stakeholders, should pay special attention to how they close emails. Here's a template of an acceptable email signature:

[Employee Name]
[Employee Title], [Company Name]
[Phone number]

Example:

Juan Dela Cruz
Information Security Officer, LT Group, Inc,
Tel. No. (+63) 1234-5678 | Mobile No. (+63) 917 1234567

4.7 E-mail Disclaimer

LTG IT will define the email disclaimer – This is a notice or warning which is added to an outgoing email and forms a distinct section which is separate from the main message. The reasons for adding such a disclaimer include confidentiality, copyright, contract formation, defamation, discrimination, harassment, privilege and viruses.

Sample Disclaimer Message:

The content of this message is confidential. If you have received it by mistake, please inform us by an email reply and then delete the message. It is forbidden to copy, forward, or in any way reveal the contents of this message to anyone. The integrity and security of this email cannot be guaranteed over the Internet. Therefore, the sender will not be held liable for any damage caused by the message.

5 ACCESS CONTROLS

The following access policies and information should be adhered within the organization;

- LTG IT as the Microsoft O365 GLOBAL ADMINISTRATOR is the overall Administrator for Exchange (E-Mail), Office Apps, SharePoint, Teams Service, Helpdesk Admin, User and Service Support Admin. The responsibilities of the roles were described on the table below.
- LTG IT as the Global Administrator has **no access** to the user's data unless provided a consent or approval from the management (Business Unit Head, Manager, IT Head). This is in the case of like incident investigation and other important business matters information needed on the said user account.
- LTG IT and employees within the organization does not have access to the information or data of their colleagues.
- The Employee / MS O365 users do not have access to the other's private conversation and access is only to the group or channels they are subscribed to.
- The Employees will only have access to the file (document, source code, spreadsheets and etc.) in MS One Drive, SharePoint and Teams when the owner of the asset allows the other users to access it (Read/Write/Edit) permission.
- In case an account is compromised, the Administrator (LTG IT) has the right to lock their account for investigation.

Admin role	Responsibility
Exchange Admin	View and manage your user's email mailboxes, Microsoft 365 groups and Exchange Online. Exchange admins can also: • Recover deleted items in a user's mailbox • Configure Archiving and Deletion Polices • Configure Anti-Spam protection • Set up "Send As" and "Send on Behalf" delegates
Global Admin	Has global access to most management features and data across Microsoft online services. Only global admins can: • Reset passwords for all users • Add and manage domains **Note:** The person who signed up for Microsoft online services automatically becomes a Global admin. *Pro tip: Giving too many users global access is a security risk and we recommend that you have between 2 and 4 Global admins.*

Helpdesk Admin	• Reset passwords • Force users to sign out • Manage service requests • Monitor service health **Note**: The Helpdesk admin can only help non-admin users and users assigned these roles: Directory reader, Guest inviter, Helpdesk admin, Message center reader, and Reports reader.
Office Apps Admin	• Use the Office cloud policy service to create and manage cloud-based policies for Office • Create and manage service requests • Manage the What's New content that users see in their Office apps • Monitor service health
Service Admin	An additional role to admins or users whose role does not include the following, but they still need to do the following: • Open and manage service requests • View and share message center posts
SharePoint Admin	Access and manage the SharePoint Online admin center. SharePoint admins can also: • Create and delete sites • Manage site collections and global SharePoint settings **Note**: Users assigned to this role will have access to all content.
Teams Service Admin	Access and manage the Teams admin center. Teams service admins can also: • Manage meetings • Manage conference bridges • Manage all org-wide settings, including federation, Teams upgrade, and Teams client settings **Note**: Users assigned to this role will have access to all content.

User Admin	• Add users and groups • Assign licenses • Manage most users properties • Create and manage user views • Update password expiration policies • Manage service requests • Monitor service health The user admin can also do the following actions for users who aren't admins and for users assigned the following roles: Directory reader, Guest inviter, Helpdesk admin, Message center reader, Reports reader: • Manage usernames • Delete and restore users • Reset passwords • Force users to sign out

6 GUIDELINES

The guidelines for improving the use of the corporate e-mail are summarized in the following:

- Users must use the signatures designed by the Company.
- Users must organize and maintain their mailboxes by deleting unnecessary messages and saving attached files on their local hard drives or on their dedicated one drive.
- All users are not allowed to copy or save corporate attachments or documents to your personal devices or storage.
- All users must verify that the data that appears in the LTG address list is correct and, if not, notify their administrators. Likewise, users must provide notification of any change to this data.
- When a reply includes the original message, the user must delete all accessory information that is not related to the content of the reply (headers, irrelevant sections, signatures, unmodified files, etc.).
- If the information to be sent is highly critical or sensitive for LTG, the user must send the information in encrypted form to avoid its manipulation or leaking during transmission.
- When replying to an email, users must avoid using "Reply to All", unless absolutely sure that "all" are the intended recipients of the reply.
- Access to other users email account and documents are prohibited without the proper consent of the owner.
- The following practices are also recommended:

  - ✓ Mail is private and individual.
  - ✓ Respect the rights of the author in all material that you reproduce.
  - ✓ When replying to a message, do not change the text.
  - ✓ Ensure that the messages replied to are directed to you.
  - ✓ Fill in the "SUBJECT" line with a short phrase that describes the content of the message.

7 RESPONSIBILITY

- The Policy shall be implemented by the ISO (Information Security Officer) / designated personnel.
- Information Security Management (ISM) is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the responsibilities identified in this policy.
- IT Department is responsible for building, configuring, operating and maintaining the corporate email facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy.
- IT Help/Service Desk is responsible for assisting users with secure use of email facilities and acts as a focal point for reporting email security incidents.
- All relevant employees are responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behavior) to comply with our information security policies.
- Internal Audit is authorized to assess compliance with this and other corporate policies at any time.

Process	R Responsible	A Accountable	C Consulted	I Informed
Proper usage of e-mail to support business related activities and complying with the Email Usage Policy	Employee	Project Manager / Department Head	IT Infra/ Information Security Office	Information Security Steering Committee (TBD)
Use of extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses	Employee	Project Manager / Unit Head	IT Infra / Information Security Office	
Appropriate protection of all e-mail correspondences	IT Infra	IT Head	Information Security Office	
The corporate e-mail shall not be used to reveal any confidential information of the company to third parties, except when carried out for strictly professional purposes and with prior consent of LTG	Employee	Project Manager / Department Head	Information Owners / Information Security Office	Information Security Steering Committee (TBD)

Inspection, monitoring and cancellation of email access or private mailbox	IT Infra	Information Security Steering Committee (TBD)	Information Security Office	Employee

8 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT GROUP, INC.

LT Group, Inc.

LTG Password Management Policy

Table of Contents

1 OBJECTIVE

This policy establishes the conditions for use of and the requirements for appropriate security for LT Group, Inc. (LTG or Company) user accounts and passwords, which are necessary:

- To protect IT systems and data
- To ensure that all users are aware of their responsibilities in effective password management.

2 SCOPE

This policy applies to all employees of LTG who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at LTG facility, has access to the LTG network, or stores any LTG information regardless of location.

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG Policy for the Use of Assets

4 POLICY STATEMENT

- Only qualified passwords shall be accepted by the system.
- Initial passwords given to users shall be replaced immediately.
- Default vendor passwords shall be replaced immediately after installation.
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed at least annually.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- After the departure of an employee, any user-level accounts for that individual must be disabled or changed to a role suitable to their status, and all system-level passwords known to that individual should be changed as soon as possible, not to exceed 3 days.
- Where SNMP (Simple Network Management Protocol) is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All user-level and system-level passwords must conform to the guidelines described in Section 6.

5 PROCEDURES

5.1 Allocation of Initial Passwords

- Initial passwords will be sent to users via e-mail whenever possible, with other communication channels (call, printed documents, etc) being used when the e-mail channel is unavailable or impractical.
- Initial passwords will be individually assigned and should be at least 8-characters long composed of a random string of alphanumeric characters. Use of a simple, generic password assigned to all users should be avoided.

5.2 Change or Reset of Passwords

- Users should change the initially assigned password as soon as possible so that the password would be easier to remember for the user.
- If the authentication module of a system has the capability to force the users to change the initial password the moment the user successfully logs on, this feature should always be activated.

6 GUIDELINES

6.1 General Password Construction Guidelines

Some of the more common uses of passwords include: user level accounts, web accounts, email accounts, screen saver protection, voice mail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. User access to the company's system and network will be configured, managed, and supported by system administrators.

Weak passwords have the following characteristics which must be avoided:

- The password contains less than eight characters
- The password is a word found in a dictionary (in any language)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "LT Group Inc", "ltg", "ltginc" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Strong passwords have the following characteristics which will be followed regardless of system-imposed restrictions:
  - Are at least eight alphanumeric characters long.
  - Are not words in any language, slang, dialect, jargon, etc.
  - Contain both upper and lower case characters (e.g., a-z, A-Z)
  - Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)\
  - Are not based on personal information, names of family, etc.

Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use any of these examples as passwords!

6.2 Password Protection Standards

Do not use the same password for LTG accounts as for other non-LTG access (e.g., personal ISP account, personal email, forums, etc.). Where possible, don't use the same password for various LTG access needs.

Do not share LTG passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential LTG information.

- Compliance with the following is required:
    - Don't reveal your password over the phone to ANYONE
    - Don't reveal a password in an email message
    - Don't reveal a password to any supervisor
    - Don't talk about a password in front of others
    - Don't hint at the format of a password (e.g., "my family name")
    - Don't reveal a password on questionnaires or security forms
    - Don't share a password with family members
    - Don't reveal a password to co-workers while away from the office
    - Don't write passwords down and store them anywhere in your office
    - Don't store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption
    - Don't use the "Remember Password" feature or the "Remember Me" on any application that contains sensitive data as defined by the Information Sensitivity Policy

If someone demands a password, refer them to this document or have them call the Information Security Office (IT Infra Security at ltginfra@ltg.com.ph).

If an account or password is suspected to have been compromised, report the incident immediately to the Information Security Office (IT Infra Security at ltginfra@ltg.com.ph) and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the Information Security personnel. If a password is guessed or cracked during one of these scans, the user will be required to change it.

6.3 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can assume the functions of another without having to know the other's password where possible.
- Require technical measures to enforce the password complexity requirements.

6.4 Pass phrases

Pass phrases are generally 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 pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:

"ThekrazyTrafficOn$*($%@)(WasnUtsThisMorning"

All of the rules above that apply to passwords apply to pass phrases.

7 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Allocation of Initial Passwords	IT Infra	IT Head	NA	Employee
Change or Reset of Passwords	Employee	Project Manager / Department Head	IT Infra	
Configuration and management of user access to the company's system and network	IT Infra (System Administrator)	IT Head	Project Manager / Department Head	Employee
Request for system administrator account for specific systems	Project Manager / Department Head	Department Head	Infra IT	Information Security Office
Approval of system administrator accounts	IT Head	Department Head	Information Security Office	Project Manager

8 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or

- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT GROUP, INC.

LT Group, Inc.

LTG Information Classification Policy

Table of Contents

1 OBJECTIVE

The objective of this policy is to define the Information Classification of LT Group, Inc. (LTG or Company)

2 SCOPE

This policy covers all types of documents used in the Company.

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System

4 POLICY STATEMENT

4.1 Responsibility of Assigning Classifications

All company employees share in the responsibility for ensuring that LTG-owned information assets receive an appropriate level of protection.

Company managers or information "owners" shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. "Owners" have approved management responsibility, but do not have property rights.

All company employees shall be guided by the information category in their security-related handling of company information.

4.2 Labelling

Where applicable, the information category shall be embedded in the information itself, preferably at the footer of the document.

4.3 Information Classification

All company information and all information entrusted to the company from third parties shall fall into one of four classifications in the table below, presented in order of increasing sensitivity.

Information Classification	Description	Examples
Public Document (P)	Information in the public domain, which have been approved for public use or distribution. Security at this level is minimal	• Company Brochures • Press Statements • Annual Reports
Internal Use Only (I)	Information not approved for general circulation outside the organization, where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to credibility/reputation. Security	• Training Materials • Attendance Sheets • Time Reports • Minutes of Meetings

	at this level is controlled, but normal.	• Organizational Charts
Confidential (C)	Information which is considered critical to the organization's ongoing operations and could seriously impede or disrupt them if made shared internally or made public. Such information should not be copied or removed from the organization's operational control without specific authority. Security should be very high.	• Salary Information • Client Information • Network Diagrams • Router Passwords • Firewall Policies • HR Confidential Documents • Finance Confidential Documents • Employee SGC's
Highly Confidential (HC)	Highly sensitive internal documents and data. Information that could seriously damage the organization if lost or made public. Information classified as Highly Confidential has very restricted distribution, mostly at the upper management level and must be protected at all times. Security at this level is the highest possible	• Investment Strategies • Company Strategic Plan

4.4 Information Handling

In each one of LTG's departments, practices, and markets, information owners shall be defined and the following aspects shall be agreed for each one of the defined classification levels:

- Who has access to the information
- Labelling
- Restrictions on electronic distribution
- Storage and safeguarding
- Disposal
- Reprimand for deliberate revelation or alteration

4.5 Handling of Digital Information

Digital media are understood to be the use of any physical media, such as files, CDs, tapes, USB's, external drives, or other removable digital devices.

4.5.1 Highly Confidential (HC)

ACCESS

- Authorization for access to information shall be centralized in the information owner.
- Only the legitimate addressee shall have access to it.
- Delegation of access to third parties by the original addressees is not permitted.
- There will be two access controls applied simultaneously:
    - Logical, imposed by the support system (e.g. permissions to objects, like for folders in the file servers)
    - Cryptographic, which facilitates the decryption password for the legitimate user only.
- All accesses will be recorded in a log (in electronic format) and the following data will be assigned:
    - Access date and time
    - Document accessed
    - Identification of the user who made access
- Physical security controls shall be implemented for the storage media of the safeguarded information.
- The procedures for authorizing access to the information shall be documented.
- The access control mechanisms shall be documented.

LABELLING

- The information must be labelled with the corresponding classification in the header or footer of each page of the document.

TRANSFER

- Transfer to third parties by the original addresses is not permitted.
- Under no circumstances shall a document be printed on a printer that can be accessed by internal or external personnel other than the personnel with permission to access it.

STORAGE AND SECURITY

- The information must be keep centralized in storage servers in which control of access to the information can be guaranteed.
- The information shall be stored encrypted without exception, by means of the cryptographic password that can only be used by the registered addresses.
- The information must be periodically safeguarded in accordance with a back-up policy that guarantees the availability of the information in the event of incidents or disasters.
- Wipe tools shall be used for destruction.

4.5.2 *Confidential (C)*

ACCESS

- Authorization for access to information shall be centralized in the information owner.
- The information owner will, at least, use a logical access control (e.g. regarding the folders on the file server) and the use of cryptographic access control is recommended.
- All accesses shall be recorded in a log (in electronic format) and the following data will be assigned:
  - Access date and time
  - Document accessed or Identification of the user who made access
- The procedures for authorizing access to the information shall be documented.
- The access control mechanisms shall be documented.

LABELLING

- The information shall be labelled with the corresponding classification in the header or footer of each page of the document.

TRANSFER

- Under no circumstances shall a document be printed on a printer that can be accessed by internal or external personnel other than the personnel with permission to access it.

STORAGE AND SECURITY

- The information must be kept centralized in storage servers, in which control of access to the information can be guaranteed.
- It is advisable to encrypt the information to be stored, both the centralized copy in the file server and the copy possibly stored in the workstations.
- The information must be periodically safeguarded in accordance with a backup policy that guarantees the availability of the information in the event of incidents or disasters.
- Wipe tools shall be used for destruction.

4.5.3 *Internal use Only (I)*

ACCESS

- There will be a logical access control.

LABELLING

- The information shall be labelled with the corresponding classification in the header or footer of each page of the document.

TRANSFER

- Not Applicable.

STORAGE AND SECURITY

- It can be located in the corporate servers and/or in the workstations of the users.
- In the event of being located in shared access servers, it will be stored in a well-defined area.

4.5.4 Public Document (P)

ACCESS

- Not applicable.

LABELLING

- Not applicable.

TRANSFER

- Not applicable.

STORAGE AND SECURITY

- Not applicable.

4.6 Handling of Non-Digital Information

4.6.1 Highly Confidential (HC)

ACCESS

- The information can only be accessed by the users authorized by the information owner or holder of the document.
- Access cannot be delegated.
- For information on paper, a physical access control shall be established with the presence of the holder.
- All accesses will be recorded on a consultation sheet under the control of the administrator or holder of the file. The following data will be recorded:
    - Access date and time
    - Document accessed or Identification of the user who made access
- Documents on paper, in general, shall not be photocopied without justification.

LABELLING

- All information containers shall be labelled with the words HIGHLY CONFIDENTIAL, with the name of the owner of the document or set of documents and the list of people authorized for access.

TRANSFER

- It shall be transferred detailing the sender and the addressee in sealed envelopes and personally delivered.

STORAGE AND SECURITY

- The information shall be stored in a physical archive (room equipped to serve as a library or archive) with robust physical access control measures (e.g. physical access card).
- In a fireproof cabinet.
- In duly labelled containers or folders.

DESTRUCTION

- The information shall be destroyed once its use is no longer necessary.
- Document shredders shall be used.

4.6.2 Confidential (C)

ACCESS

- The information shall only be accessed by the users authorized by the owner or holder of the document.
- Physical access control shall be established (the presence of the owner is not necessary) over the file.
- All accesses shall be recorded on a consultation sheet under the control of the administrator or holder of the file. The following data will be recorded:
    - Access date and time
    - Document accessed
    - Identification of the user who made access
- The documents can be photocopied if the owner or holder approves it.

LABELLING

- All information containers shall be labelled with the word CONFIDENTIAL, with the name of the owner of the document or set of documents and the list of people authorized for access.

TRANSFER

- It shall be transferred detailing the sender and the addressee in sealed and lacquered packets and personally delivered.

STORAGE AND SECURITY

- The information shall be stored in a physical archive (room equipped to serve as a library or archive) with robust physical access control measures
- In duly labelled containers or folders.

DESTRUCTION

- The information shall be destroyed once its use is no longer necessary.
- Document shredders shall be used.

4.6.3 Internal Use Only (I)

ACCESS

- Special measures are not proposed for access to documents on paper, unless the file is in an area controlled by the information owner, holder, or addressee and not directly accessible by non-LTG personnel.

LABELLING

- Not Applicable

TRANSFER

- Not Applicable

STORAGE AND SECURITY

- The information shall normally be stored under lock and key. For example, in a personal cabinet belonging to the owner, holder or addressee.

DESTRUCTION

- Not Applicable

4.6.4 Public Document (P)

ACCESS

- Not applicable

LABELLING

- Not applicable

TRANSFER

- Not applicable

STORAGE AND SECURITY

- Not applicable

DESTRUCTION

- Not applicable

5 RACI

The following table shows the responsibility and accountability matrix for the information Classification Policy.

Process	R Responsible	A Accountable	C Consulted	I Informed
Classification of Information Assets	Unit Head	Director	IT Infra / IT Security Team	Employees
Control to access of Information	Information Owner	Unit Head	IT Infra / IT Security Team	Employees
Labelling of information Assets	Information Owner	Unit Head	IT Infra / IT Security Team	Employees
Transfer	Document Holder	Information Owner	Administrative Services/ IT Infra	Employees
Storage and Labelling	Information Owner	Unit Head	IT Infra / IT Security Team	Employees

Destruction	Information Owner	Unit Head	IT Infra / IT Security Team	Employees

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Internet Usage Policy

Table of Contents

1 OBJECTIVE

To define the policies and procedures for accessing the Company IT Network and/or accessing the Internet through the LT Group, Inc. (LTG or Company) IT Network.

2 SCOPE

This policy applies to all personnel and visitors with access to the Internet and related services through the Company network infrastructure. Internet-related services include all services provided with the TCP/IP protocol, including, but not limited to:

- electronic mail (e-mail),
- file transfer protocol (FTP), and
- world wide web (WWW) access

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG Policy for Use of Assets
LTG E-Mail and Collaborative Tools Policy

4 POLICY STATEMENT

Access to the Internet is specifically limited to activities in direct support of official Company business, including research and studies.

Employees shall be responsible in practicing acceptable usage of the company Internet.

- Internet access shall not be for any illegal or unlawful purpose. Examples of these are the transmission of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful materials.
- The Company e-mail or other messaging services shall not be used to harass, intimidate or otherwise annoy another person.
- The Internet shall not be accessed for private, recreational, or any non-company related activity. Posting of Company's Information and other work-related matters to any kind of social media is strictly prohibited.
- The Company's intranet or internet connections shall not be used for commercial or political purposes.
- Employees shall not use the Company network for personal gain, such as selling access of a Company user login ID. Internet access through the Company network shall not be for or by performing unauthorized work for profit.
- Users shall not attempt to circumvent or subvert security measures on either the Company's network resources or any other system connected to or accessible through the Internet.
- Company employees shall not use Internet access for interception of network traffic for any purpose other than engaging in authorized network administration.
- Company users shall not make or use illegal copies of copyrighted material, store such material on Company equipment, or transmit such material over the Company network
- Download of copyrighted materials and unlicensed software are strictly prohibited.

- Download of movies, TV series, videos, music, and images that are non-business related are strictly prohibited.

5 GUIDELINES

Visitors requiring access to the Internet will be provided with guest accounts connection. Employees accountable for guests may coordinate with IT Infra.

6 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Acceptable usage of the company internet	Employee	Project Manager/Department Head	Information Security Office	NA
Requesting for the Guest Account for Visitors requiring the use of the internet	Employee	Project Manager/ Department Head	IT Infra	Information Security Office
Setup of Internet for Visitors	IT Infra	IT Head	Information Security Office	Employee / Project Manager / Department Head

7 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Network Access Policy

Table of Contents

1 OBJECTIVE

This is to ensure the availability and integrity of LT Group, Inc. (LTG or Company)'s network with regards to the risks associated with the connection of new elements or resources.

2 SCOPE

This policy is applicable to LTG network resources and infrastructure and all users of the network are subject to the terms of this document.

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG Information Classification Policy
LTG Policy for the Use of Assets

4 POLICY STATEMENT

LTG reserves the right to control, segregate and limit the Internet service and network accesses to users and resources for reasons of security or network performance.

LTG internal network must be protected from unauthorized accesses and outside threats. All network devices and interconnecting equipment shall be configured properly and protected.

The computers and the network provide access to internal and external resources in addition to communication with users around the world. This privilege implies certain responsibilities for the users, who must respect the rights of other users, the integrity of the system and of its physical resources, and applicable laws and regulations.

The user commits to respecting the rules and regulations established by LTG and by other bodies and institutions with which the user might interact within the framework of national and international communications.

Network utilization and activity shall be monitored, and logs shall be kept for records.

Inappropriate use will be sanctioned by the removal of access and the application of the corresponding disciplinary actions.

5 GUIDELINES

5.1 Mandatory Rules

- When an area requires the installation of an element or hardware with connection to LTG's internal network, the manager of the area, the project manager, or the user responsible for the action must submit an LTG network resource connection request to the IT Infra Security Team.

Under no circumstance it is permitted to make the connection without the consent of the immediate superior and approval from the IT department.

- Once the resource has been connected, the person who requested it and the manager of the project and/or area shall guarantee the correct use and updating of the connected elements in accordance with the compulsory compliance and good usage regulations established by Management.

- All connections between units in the LTG network and external units shall apply the security measures required to prevent external attacks and be initially and periodically supervised by LTG IT Infra Security.

- In the case of external connection to the Internet from the LTG network, it is strictly forbidden to use any other means (for example, wireless modems) other than those provided by LTG IT Infra Security.

- All network devices shall be correctly configured to ensure correct operation. Default manufacturer passwords must be replaced by a complex password for protection from unauthorized access.

- Network protection devices shall be installed to prevent outside threats and attacks. Built-in protection features of interconnecting devices must be configured.

- Networks within LTG premises shall be segregated according to its functions and connection requirements to maintain confidentiality of important resources that can be accessed within a network.

- For security and network maintenance purposes, authorized individuals within LTG IT Infra shall monitor equipment, systems, and network traffic at any time. Access rights of employees at storage facilities (e.g. network drives, document repositories) shall also be reviewed periodically.

- LTG IT Infra shall provide a reasonable level of privacy. However, all usage of computing resources shall be logged. These logs are to be maintained by the LTG IT Infra.

5.2 Acceptable Use

- Once the resource has been connected, the user is obliged to use it exclusively in relation to LTG's activity and any other unauthorized commercial and/or private use is strictly forbidden.

- The owner of the account and/or the person responsible for the resource must ensure its maintenance and good usage and is subject to the sanctions established by LTG in each case upon detection of an inappropriate or forbidden activity.

- Depending on whether the incident or inconvenience caused to other users or to the service seriously and immediately affects the system, LTG IT Infra Security will have the power to take the measures necessary to immediately restore correct service. These measures include:

    - Disconnection of the users of the computers
    - Disabling the network access of the resource or group of resources generating the malfunction or breach of the security rules

5.3 Unacceptable Use

- Physical damage to the network infrastructure and resources.

- Connection, disconnection or relocation of resources or changes to their configuration without informing LTG IT Infra and obtaining authorization from their respective supervisor.

- Installation of remote access devices and cards, modems, ISDN (Integrated Services Digital Network), routers or any other communications device in LTG's computers or networks without the knowledge of LTG IT Infra.

- Installation of communications units for exchanging information between computers in LTG's network and external computers.

- Use of LTG's network or computers to gain unauthorized access to a computer.

- Deliberately carrying out any act that interferes with the correct operation of the computers, terminals, peripherals, communications network, etc.

- Installing or running at any point in the computer network (computers or network software) programs or files that deteriorate or excessively increase the load at any point in the network, endangering other users or the performance of the network. This includes programs known as computer viruses, all types of test and experiment, etc.

- Installing or running at any point in the computer network (computers or network software) programs or files that attempt to discover information other than that of the user, in any element of the network. This includes sniffers, port scanners, etc.

- Disabling and re-configuring the installed and built-in protection (i.e. antivirus, software firewalls, etc) on computing systems.

- Attempting to bypass data or computer security systems.

- Violations of data protection laws, program licenses and copyright.

- Executing any form of network monitoring, which will intercept data not intended for the employee's host.

- 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.

  Some of the above activities will not be considered incorrect use of LTG's computer resources if they are authorized by LTG IT Infra and carried out by this department's technical team in order to test or increase the IT security of the network.

6 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Request for the installation of an element or hardware with connection to LTG's internal network	Project Manager / Department Head	Unit Head	IT Infra / Information Security Office	Information Security Steering Committee (TBD)
Responsible use of network resources and all elements connected to the LTG internal/ corporate network	Employee	Project Manager / Unit Head	IT Infra / Information Security Office	Information Security Steering Committee (TBD)
Protection of the LTG internal network from unauthorized access and external threats	IT Infra Security	IT Head	Information Security Office	Information Security Steering Committee (TBD)/Asset Owner
Monitoring of network utilization and activities, including the maintenance of logs	IT Infra	IT Head	Information Security Office	Information Security Steering Committee (TBD)/Asset Owner
Configuration of all network devices to ensure correct operation	IT Infra Security	IT Head	Asset Owner	Information Security Office

Ensuring the segregation of networks within LTG premises according to its functions and connection requirements	IT Infra Security	IT Head	Asset Owner	Information Security Office

7 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Physical Access Policy

Table of Contents

1 OBJECTIVE

The objective of this document is to set the proper guidelines that will:

- Provide the employees of LT Group, Inc. (LTG or Company) a safe work environment.
- Provide the employees the proper usage guidelines for the access security system.
- Create a vehicle through which the safety and security recommendations, complaints and concerns are reviewed for action by Administrative Services Unit.

2 SCOPE

This policy covers all employees, subcontractors (project hire, sub-contractual employees, janitors, messengers, and security personnel).

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG Visitor Policy
LTG Office Layout

4 BRIEF DESCRIPTION

This document defines the physical access to the office policy, the location of access doors with security locks and the limitations of access of LTG personnel.

5 ROLES AND RESPONSIBILITIES

5.1 Administrative Services

- Monitor the CCTV and ensure the compliance of the policy.
- Inform IT &HR of reported lost ID/Access Card.
- Issue temporary access cards.
- Report to HR offenses committed by an employee for records purposes.

5.2 IT Services

- Deactivate lost ID/Access Card

5.3 Human Resources

- Issue new ID/Access Card.
- Re-issue of new ID/Access Card.
- Record offenses committed by an employee for sanction purposes as described in this document.

5.4 Finance

- Administer salary deduction of the cost of new ID/Access Card from concerned employee.

6 GENERAL GUIDELINESS

6.1 Issuance of ID/Access Card

Company ID cards will serve as the access cards for the employees. All employees will be issued an ID/Access card.

6.2 Restrictions

- All valid cardholders will have access to all doors except the Data Center from 8am to 5pm from Mondays to Fridays.
- Non-working hours from Monday to Friday, from 5:01pm to 7:59am Saturday to Sunday (whole day) will have restricted access as follows:
    - 4th Floor PNB Makati Center assigned employees will be restricted to the 4th floor area only.
    - 11th Floor BGC Bench Tower assigned employees will be restricted to the 11th Floor area only.
    - All employees assigned outside PNB Makati Center will be restricted to any LTG office (Makati Office and BGC Office)
    - All Management Committee Members will have access to all doors at all times except the Data Center and Executive Office.
    - All Business Developers and will have access to the 4th Floor PNB Makati Center except the Executive Office and Data Center.
- Anti-passback feature will be activated for all doors except the Executive Area and Data Center.
- Tailgating and piggybacking is strictly prohibited.
- Overtime Work in restricted floor after office hours will follow the following procedures:
    - Employees who will need to work overtime to a restricted floor after working hours must inform Administrative Services through an email addressed to adminoffice@ltg.com.ph
    - Administrative Services will instruct the Security Guard on duty to assist requesting employee for the access in & out of said floor.
- Visitors must be escorted in and out of the work premises at all times as per LTG's Visitors Policy.

6.3 Lost ID/Access Card

- Employees that lose or damage their ID/access card will be issued a temporary pass up to such a time when their new ID/access card is issued.
- Employee can proceed to the 4th Floor Reception Area and sign the log sheet provided. Administrative Services through the Security Guard will issue the temporary pass.
- Employees must immediately inform Administrative Services through an email to adminoffice@ltg.com.ph of the loss or damage of their ID/access card.

- Administrative Services will inform IT Infra to deactivate said ID/access card.
- Administrative Services will inform HR for the issuance of a new ID/access card.
- Employee will pay the replacement cost of the ID/access card through salary deduction.
- Upon issuance of the new ID/access card, the temporary card will be surrendered to HR. Failure of the employee to surrender the temporary card to HR will be charged the cost of the card through salary deduction.
- HR shall inform Administrative Services and IT to immediately deactivate the temporary card if an employee fails to surrender the temporary card assigned to him/her.
- HR will turn over the returned temporary card to Administrative Services

6.4 New Employees

- New employees will be issued a temporary ID/access card by HR.
- The temporary card will be surrendered to HR once he/she receives his/her new valid ID/access card.

6.5 ID/Access Card Left at Home

This pertains to employees who report for work without their ID/access card on a temporary basis.

- Employee, who report for work without their ID/access card, will have to proceed to the 4th Floor Reception Area.
- Employee must sign the log sheet provided.
- After signing, the Security Guard on duty will issue a temporary pass that will be valid for one day only.
- Security Guard will note the temporary pass number in the log sheet.
- Employee must surrender the temporary pass at the end of his/her working hours.
- An employee who fails to surrender the temporary pass on the same day issued will be subject to sanction and an offense will be recorded.
- Temporary cards not returned on the same day will be deactivated on the following day.
- Security Personnel will turn-over to Admin the records of unreturned Temporary ID and the name of employee/s it was issued. Admin will report to Immediate Manager for applicable Corrective Actions based on the Employee Manual.

6.6 Sanctions For Not Having An ID/Access Card

This will be considered a Minor offense and shall progress accordingly and based on the gravity of the violation. Please refer to the table below on the Classification of Offenses and Implementation of Corrective Action in section 9.

7 AREAS WITH SECURITY ACCESS CONTROL SYSTEM

- LTG Office PNB Makati Center 4th Floor – Main Door
- LTG Office PNB Makati Center 4th Floor – Pantry Door
- LTG Office PNB Makati Center 4th Floor – Data Center Door
- LTG Office BGC Bench Tower 11th Floor – Main Door

8 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Enforcement of Overall Physical Security	Administrative Services Staff	Administrative Services Head	Information Security Office	Employees
Identifying Employee Access Rights	Project Manager/Unit Head	Unit Head	IT Infra / HR / Administrative Services	Information Security Office
Keeping ID Cards and wearing Them	Employee	Project Manager/Unit Head	NA	NA
No Tailgating / Piggybacking	Employee	Project Manager/Unit Head	Administrative Services	Information Security Office
Escorting of Visitors	Employee	Project Manager/Unit Head	Administrative Services	Information Security Office
Monitoring the CCTV	Security Staff	Administrative Services	IT Infra	Information Security Office
Reporting of Lost/Damaged ID	Employee	Project Manager/Unit Head	Administrative Services	Information Security Office
Issuance of Temporary ID Card	Administrative Services Staff	Administrative Services Head	IT Infra / HR	Employee
Surrendering of Temporary Card	Employee	Project Manager/Unit Head	Administrative Services/HR	Information Security Office
Deactivation of ID Card	IT Infra	IT Head	Administrative Services / HR	Employee / Information Security Office

Issuance of New/Replacement ID Card	HR	HR Head	Administrative Services / HR	Employee
Tracking of Offenses or Implementation of Sanctions	HR	Immediate Supervisor	Administrative Services / Finance	Information Security Office

9 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Policy for the Use of Assets

Table of Contents

1 OBJECTIVE

To outline the policies that governs the use of information assets owned and/or controlled by LT Group, Inc. (LTG)

To protect employees, consultants, licensees, lessees, vendors, clients, and affiliates from any exposure to information security risks related to the use of information assets and processing facilities.

2 SCOPE

This policy applies to all types of information assets and processing facilities that are owned and/or controlled by LTG, regardless of location, such as:

- Proprietary Information and Data residing on corporate systems such as Press Statements, Annual Reports, confidential documents like Salary Information, Client Information, Network Diagrams, Router Passwords, Firewall Policies, HR Confidential Documents ,Finance Confidential Documents and Investment Strategies.
- User Access (accounts and passwords)
- Computer Equipment, such as desktop computers and laptop computers
- Removable Media, such as external hard drives, thumb drives, memory cards, etc.
- Network Access (LAN and WAN)
- Other equipment, like printers, photocopy machines, televisions, etc.
- E-mail and Internet

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG E-Mail and collaborative tools Policy
LTG Internet Usage Policy
LTG Secure Workstation Policy
LTG Disposal of Assets

4 POLICY STATEMENT

4.1 General Use and Ownership

The use of company-owned equipment shall be restricted to business purposes and users must be aware of and accept the terms and conditions of use, especially the responsibility for the security of information held on such equipment.

4.2 Data Ownership

All data created in or using company-owned equipment shall be owned by the author, but shall remain the properties of LTG and shall be under the custody of LTG IT Infra.

4.3 Personal Use

Games are strictly prohibited.

Users shall be responsible for exercising due diligence regarding the reasonable use of the e-mail and the Internet.

- Use of the company e-mail shall be governed by the LTG E-Mail and collaborative tools Policy
- Use of the company Internet shall be governed by the LTG Internet Usage Policy

4.4 User ID's and Passwords

All employees shall have individual user IDs and passwords to maintain accountability. Sharing of user ID's and passwords are not allowed.

Employees shall be responsible for keeping user accounts and passwords secure and confidential.

Revealing of an employee's account password to others or allowing the use of the company account by others shall be strictly prohibited. This includes family and other household members when work is being done at home.

4.5 Equipment and Workstation Security

Employees shall be responsible for the security of company-issued equipment assigned to them and the sensitive data stored in that equipment.

All equipment being pulled out of office premises shall be supported by proper documentation and proper authorization.

Users shall be responsible for securing their workstations according to the **LTG Secure Workstation Policy**.

All users shall shut down their respective workstations at the end of the day, unless needed for the running of processes related to project operations. In such cases, the employee shall obtain proper authorization and the workstation shall be locked.

4.6 Use of Laptops Mobile Devices, and Removable Media

Line Management (project managers and up) shall recommend the issuance of laptops and mobile devices to employees. IT head shall have the final authorization for the issuance of laptops and mobile devices to designated employee.

Employees shall report any loss of mobile computers and telecommunication equipment immediately.

The use and transit of removable media shall be strictly governed by the defined Removable Media Handling Guideline.

4.7 Security of Proprietary Information

All information contained in the Company Intranet are classified as confidential and are intended for staff use only, while information in the Company Internet site are classified as public.

All users shall obtain proper authorization through a formal authorization process before releasing proprietary information to external parties. The integrity of such information shall be protected after its release.

Exchange of proprietary information using communication facilities, including but not limited to voice, data, facsimile, and video communication, shall be controlled.

4.8 Use of Personal Equipment

Use of personal computers and removable media for work-related matters shall not be allowed unless specifically authorized by line management (Project Manager).

4.9 Protection against Viruses and Malware

All company-owned computer equipment shall be installed with the standard anti-virus software and its corresponding up-to-date virus database.

Users shall ensure that the anti-virus software is always updated with the latest virus database.

4.10 Unacceptable Use of Assets

The following activities shall be strictly prohibited:

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 software products or other products that are not appropriately licensed for use by LTG IT Infra.

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.

3. Export of software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan, e-mail bombs, etc.).

5. Use of computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws within the organization and locality.

6. Making fraudulent offers of products, items, or services originating from any account.

4.11 Responsibility of IT Infra

LTG IT Infra shall be responsible for:

- Ensuring that users are granted appropriate access rights.
- Ensuring that computer facilities are being used to support business operations.
- Ensuring that all computer equipment are installed with licensed software, the company standard anti-virus software and an up-to-date virus database.
- Ensuring that exchange of proprietary information using the company communication facilities are controlled.
- Monitoring network activities as appropriate
- Following standard procedures and guidelines to enforce the policies stated in this document.

5 GUIDELINES

All company owned mobile phones must be secured with a personal PIN for purposes of safekeeping information stored in the device.

Persons who are issued with mobile devices should be made aware of the information security issues relating to mobile computing facilities.

6 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
No games shall be installed or played in company-owned assets	Employee	Project Manager / Unit Head	IT Infra / Information Security Office	Information Security Steering Committee (TBD)

Security and confidentiality of individual ID's, accounts, and passwords	Employee	Project Managers/Unit Head	IT Infra / HR	Information Security Office
Security of assigned equipment and reporting of the loss of mobile computers and telecommunication equipment immediately	Employee	Project Managers/Unit Head	Administrative Services	Information Security Office
Shut down of workstations at the end of the day	Employees	Project Managers/Unit Head	Administrative Services	Information Security Office
Request for the issuance of laptops, mobile devices, and employees	Project Manager	Unit Head	IT Infra / Administrative Services	Information Security Office
Obtaining proper authorization through a formal authorization process before releasing proprietary information to external parties	Employee	Project Manager/Unit Head	Information Asset Owner	Information Security Office /Information Security Steering Committee (TBD)
Control of the exchange of proprietary information using communication facilities, including but not limited to voice, data, facsimile, and video communication	IT Infra	IT Head	Information Security Office	Employees
Non-use of personal computers and removable media for work-related matters, unless specifically authorized by line management.	Employee	Project Manager/Unit Head	IT Infra/ Information Security Office	Information Security Steering Committee (TBD)

Authorization of the use of personal equipment for work-related matters	Unit Head	Information Security Office	IT Infra	Employee
Installation of the standard anti-virus software and its corresponding up-to date virus database on all company-owned computer equipment	IT Infra	IT Head	Information Security Office	Employee
Ensuring that the anti-virus software is always updated with the latest virus database	Employee	Project Managers/Unit Head	IT Infra/ Information Security Office	NA
Ensuring that users are granted appropriate access rights	IT Infra	IT Head	Project Managers/Human Resources	Information Security Office
Ensuring that computer facilities are being used to support business operations	IT Infra	IT Head	Information Security Office	Information Security Steering Committee (TBD)
Ensuring that all computer equipment are installed with licensed software	IT Infra	IT Head	Information Security Office	Information Security Steering Committee (TBD)

Monitoring network activities as appropriate	IT Infra	IT Head	Information Security Office	Information Security Steering Committee (TBD)

7 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or

- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Disposal of Assets Policy

Table of Contents

.

1 OBJECTIVE

To set the policies to be enforced in the proper disposal of information assets owned by LT Group, Inc. (LTG).

2 SCOPE

This policy governs the disposal of all information assets that contain sensitive and confidential information, specifically:

- Documents (whether electronic or printed on paper)
- Hard Drives (both internal or external)
- Removable Media (including external hard drives, memory cards, USB drives, optical disk, floppy disk)

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG Policy for the Use of Assets
LTG Information Classification Policy
LTG E-mail and Collaborative Tools Policy
LTG Internet Usage Policy
LTG Secure Workstation Policy

4 POLICY STATEMENT

4.1 Disposal of Non-Public Documents

Non-public documents shall be disposed of securely and safely when no longer needed using formal procedures and guidelines. Refer to the **LTG Data Privacy Policy Section 11 Disposal and Destruction.**

The company shall provide facilities for the proper disposal of non-public documents.

4.2 Re-Use and Disposal of Devices and Storage Media

Devices with sensitive information shall be physically destroyed or the information shall be destroyed, deleted or overwritten through techniques preventing from the retrieval of the original information, instead of using normal deletion or formatting techniques.

Media shall be disposed of securely and safely when no longer needed using formal procedures and guidelines.

All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

.

5 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Enforcement of Policy for the Disposal of Non-public Documents	Administrative Services Staff	Administrative Services Head	Information Security Office	Information Security Steering Committee
Enforcement of Policy for the Disposal of Devices and Storage Media	IT Infra	IT Head	Information Security Office	Information Security Steering Committee
Disposal of Non-Public Documents	Employee	Project Manager/Unit Head	Administrative Services / Information Security Office	Employee
Ensuring that Sensitive Data and Software has been removed or securely overwritten prior to disposal or re-use	IT Infra	IT Head	Information Security Office	Information Security Steering Committee / Employee
Secure Disposal of Storage Media and Devices	IT Infra	IT Head	Information Security Office	Information Security Steering Committee

6 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

.

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Secure Workstation Policy

Table of Contents

1 OBJECTIVE

To establish the rules, which control the presence of LT Group, Inc. (LTG)'s information assets within the environment of the employee in periods of inactivity.

2 SCOPE

This document is applicable to all assets whose confidentiality or integrity might be threatened as a consequence of their uncontrolled public exposure.

3 REFERENCE

The latest edition/review of the following documents will be used as a reference in the application of this manual:

ISO/IEC 27001:2013 Information Security Management System
LTG Policy for the Use of Assets
LTG Removable Media Handling Guideline

4 POLICY STATEMENT

All LTG employees, both permanent and temporary, will follow Secure Workstation rules, so that storage, documentation and information devices are protected when the employee leaves the workstation.

These rules are known to all LTG employees as part of their information security training and awareness, and they are as follows:

- Documentation, reports and information technology media such as tapes or disks must be kept under lock and key, especially outside working hours.
- Sensitive or critical information must be kept in a safe place, under lock and key, when not required, especially when the office is empty.
- Workstations, terminals must have authentication, password or other access control mechanisms and automatic blocking in the event of being left unattended.
- Mailboxes, fax and telex machines must not be left unattended if they are not protected.
- Printed sensitive or classified information must be immediately removed from printers
- All users will configure their screen saver with password protection so that it is activated after 5 minutes of inactivity.
- Offices and rooms must be closed when they are not in use.
- Desks must be left free of paperwork after working hours. Confidential information must be kept under lock and key in the event of any absence from the workplace.
- Handling of LTG Confidential documents shall be governed by the defined policies in Section 4.5 and 4.6 under LTG Information Classification Policy.

5 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Enforcement of Policy	Administrative Services Staff	Administrative Services Head	Information Security Office	NA
Securing Workstations	Employee	Project Manager/Unit Head	Administrative Services	Information Security Office
Securing documentation, reports, and media, such as USB's, and external drives.	Employee	Project Manager/Unit Head	Administrative Services / IT Infra	Information Security Office
Authentication, password, or access control mechanisms for workstation, terminals and printers	IT Infra	IT Head	Information Security Office	Employees
Securing mailboxes and fax, printer machines,	Administrative Services Staff	Administrative Services Head	Information Security Office	Employees
Protecting photocopiers against unauthorized use outside of working hours	Administrative Services Staff	Administrative Services Head	Information Security Office	Employees / Security Staff
Locking of screens and clearing of desks when leaving work area unattended	Employee	Project Manager/Unit Head	Administrative Services / IT Infra	Information Security Office

6 SANCTIONS

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Visitors Policy

Table of Contents

1 OBJECTIVE

To set the policies that will:

- Provide, and maintain a safe work environment for the employees of in LT Group, Inc (LTG).
- Identify and authorize all persons aside from employees entering the premises.
- Monitor the use and effectiveness of security resources.
- Create a vehicle through which safety and security recommendations, complaints and concerns are reviewed for action by Administrative Services Unit.

2 SCOPE

These policies, guidelines and procedures cover all clients, vendors, suppliers, contractors, partners and guests of LTG employees.

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System
LTG Physical Access Policy

4 POLICY STATEMENT

4.1 Visitors

- The LTG employee shall be responsible for his/her visitor/s actions while in the premises of LTG
- Visitors shall be escorted or guided at all times
- Former employees may visit the LTG facilities for as long as they are not included in the Black List/Denied Access List of LTG.
- Former employees shall be considered as Visitors.
- All LTG employees shall have the right to question any individual not accompanied by an LTG employee and can escort him/her off the work area.
- Visitors are not permitted to take still or video photography inside the LTG premises without prior written approval by the LTG Administrative Services Admin.
- Armed bodyguards are not permitted to enter the LTG work area unless prior arrangements have been made with Administration.
- Applicants for employment are not allowed to bring in their personal laptops inside LTG office premises.
- At no time will an applicant be allowed to have access around PNB Makati Center 4th floor area including the pantry except for the reception waiting area and interview room.
- Long staying personal guests are discouraged to stay in the office premises for more than 30 minutes unless prior approval is requested to the LTG Administrative Services Admin.

4.2 Delivery and Miscellaneous

- Delivery of personal packages/materials directly to employees inside the work areas shall not be allowed.

- Safekeeping of personal items of an employee at the reception shall not be allowed.
- Deliveries of individual food orders are NOT permitted in LTG premises.
- Lobby guards/receptionist are prohibited from accepting money to pay for deliveries or for accepting items from delivery persons on behalf of the employees.
- Bulk deliveries of food only for official company functions are permitted with advanced arrangement with Administration.
- Delivery persons not wearing a PNB Makati Center Visitors ID shall not be allowed access inside the LTG premises.
- Employees are discouraged to host personal functions inside the premises of LTG.

5 GUIDELINES

5.1 Visitors

- The LTG employee is responsible for ensuring that the visitor/s has/have no access to unauthorized information or areas.
- Security Staff / Receptionist shall ensure that the applicant/s display the PNB Makati Center or LTG Visitor's Pass at all times.
- LTG Employee may bring his/her personal guest/s to the Floor Pantry. However, the LTG employee must stay with his/her guest at all times until they depart from the office premises. At no time will a personal guest be left unattended while in the office premises.
- The Unit Head will have the responsibility to inform the visitors (LTG Employees from Affiliated Company) on the office policies and also the return of the access card to Administrative services at the end of their visitor's visit.
- Visitor's access card restriction will have the same as an LTG employee.

5.2 Delivery and Miscellaneous

- All delivered official items (packages, letters, etc) shall be received by the receptionist or employee concerned at the 4th Floor.
- The LTG employee concerned must always accompany the delivery personnel. At no time can the delivery personnel be left unattended.
- The lobby guard/receptionist shall ensure that the delivery person shall display the PNB Makati Center Visitor's Pass at all times.
- Administrative Services must be informed of all deliveries of office supplies for replenishment of office supplies stocks or project related supplies.

6 PROCEDURES

6.1 Visitors

6.1.1 Official Visitors / Clients /Partners

- All visitors shall proceed directly to the PNB Makati Center reception desk located at the lobby for proper registration and issuance of the appropriate Visitor's pass.
- Visitor/s shall then proceed to LTG Office 4th Floor reception desk and will be required to log on the LTG Visitor's log book indicating their name, company, address, contact numbers, purpose of visit and LTG employee they are visiting. If guest is bringing in a laptop, he must register his/her laptop by filling out the Serial number of his laptop in the column provided in the Visitors Log Book.
- Lobby guard shall ensure that visitor/s display the PNB Makati Center Visitor's Pass at all times.
- Lobby guard/receptionist shall then inform the LTG employee via telephone of the visitor's name. Unverified guests shall not be allowed to enter the premises.
- LTG employee or representative shall proceed to the lobby to verify the identity of the visitor/s, provide access to the work area and escort the visitor/s to the appropriate office or meeting rooms. At no time should the visitor/s be left on their own to wander around the work area/s. An LTG employee must at all times accompany the visitor/s while inside the work areas.
- If the LTG employee is not available, the visitor may stay at the lobby waiting area for 30 minutes. After 30 minutes, should the LTG Employee still not be available the Lobby guard/receptionist should inform Administration (Building Admin).

6.1.2 Former Employees

- Former employees shall be considered as Visitors and must follow the same procedures in section 6.1.1.

6.1.3 VIP Visitors

- LTG employee must notify Administration (Building Admin) in advance of any high profile, high ranking government official or LTG and Subsidiaries Executive Guests in order to arrange the waiver of the first three procedures under section 6.1.1.
- The VIP guest/s must still be escorted inside the secured office area by an LTG employee.
- LTG Administrative Services Staff will coordinate with PNB Makati Center Administration (Building Admin) on the waiver of their Visitor's Registration Policy at the Ground Floor.

6.1.4 LTG Employees and Affiliated Companies

- All LTG employees from affiliated companies (e.g. Asia Brewery, PNB, PAL, Tanduay Distillers Inc., etc.) shall be issued a Visitor's access card upon the request of the hosting department head and approved by HR-Admin Head.

- Visitor's access card must be surrendered back to Administrative Services Unit at the end of their visit.

6.1.5 *Applicants for Employment with Scheduled Interview*

- Human Resources shall furnish daily to the 4th floor Receptionist / Security Staff a list of applicants scheduled for interview and the assigned Interview Room.
- All applicants shall proceed directly to the PNB Makati Center reception desk located at the lobby for proper registration and issuance of the appropriate visitor's pass.
- Applicant shall then proceed to LTG 4th floor reception desk and will be required to register or Log in Visitor's Log book by indicating their name, address, contact numbers, purpose of visit and LTG employee they are visiting.
- Receptionist shall cross check the list of applicants submitted by HR and inform HR employee via telephone of the applicant's presence.
- Receptionist shall request the applicant to proceed to the interview room assigned to him/her.

6.1.6 *Personal Guest of LTG Employees*

- Guests shall proceed to the PNB Makati Center reception desk located at the lobby for proper registration and issuance of the appropriate visitor's pass.
- Guest shall then proceed to LTG Office at 4th floor reception desk and will be required to register in the Visitor's Registration Sheet / Log Book by indicating their name, address, company, contact numbers, purpose of visit and LTG employee they are visiting.
- Receptionist will inform LTG employee of his/her guest via telephone.
- LTG employee will meet his/her guest at the 4th Floor Reception Waiting Area only.

6.2 Delivery and Miscellaneous

6.2.1 *Delivery of Packages/Materials*

- The receptionist shall receive and record the official delivered items in the log book before turning over the item to the proper person concerned. The addressee or recipient shall be required to sign the logbook to signify the receipt of the item.
- For personal items, the receptionist shall notify the addressee via phone of the package to claim the item. If the addressee is not available and no employee in the office of the addressee is willing to accept the item, then the item shall be returned to the person delivering them.

6.2.2 *Delivery of Office Supplies*

- Administrative Services will prepare all the necessary gate passes in order to secure all the necessary approvals from LTG and PNB Makati Center Administration.
- For small orders, the deliveries can be received by the receptionist who will have the responsibility of informing the employee concerned for the immediate pick up of the supplies.

- For bulk orders, the receptionist must inform the employee concerned of the delivery and it will be the responsibility of the employee to accompany the delivery personnel to the proper area of storage of the supplies.

7 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Enforcement of the policy	Administrative Services Staff / Security Staff	Administrative Services Head	Information Security Office	Employees
Responsible for visitors	Employee	Project Manager / Unit Head	Administrative Services	Information Security Office / Security Staff
Maintenance of the Black List/ Denied Access List of LTG	Administrative Services Head	Information Security Steering Committee	Information Security Office	Information Security Office / Security Staff
Proper registration of visitor	Receptionist/ Security Staff	Administrative Services Head	Security Staff	Information Security Office
Handling of VIP Guests	Administrative Services Head	Information Security Steering Committee	Information Security Office	Administrative Services Staff
Ensure that Visitor has a visitor pass	Employee	Project Manager / Department Head	Administrative Services / Security Staff	Information Security Office
Visitor laptop registration	Receptionist/ Security Staff	Administrative Services Head	Security Staff	Information Security Office/Employee
Responsibility for applicants with scheduled interview	HR Staff	HR Head	Administrative Services	Information Security Office/Security Staff
Responsibility for personal guests	Employee	Project Manager / Department Head	Administrative Services / Security Staff	Information Security Office
Responsibility for deliveries	Employee	Project Manager / Department Head	Administrative Services / Security Staff	Information Security Office

8 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Disaster Recovery Policy

Table of Contents

1 OBJECTIVE

This policy defines the need for management to support ongoing disaster planning for LT Group, Inc. (LTG or Company)

2 SCOPE

This policy applies to the LTG management and technical staff including third party service providers.

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System

4 POLICY STATEMENT

- LTG must create and implement a **Disaster Recovery Plan** ("DRP").
- The DRP must be periodically tested and the results should be used as part of the ongoing improvement of the DRP.
- The DRP, at a minimum, will identify and protect against risks to critical systems and sensitive information in the event of a disaster.
- The DRP shall provide for contingencies to restore information and systems if a disaster occurs. The concept of disaster recovery includes business continuity.
- LTG disaster recovery planning must ensure that:
    - an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience, and competence;
    - personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security are nominated;
    - documented plans, response and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.
- The LTG DRP must include at a minimum, the following elements:
    - Business impact analysis, including risk assessment, Information Resource asset classification, and potential disruption to stakeholders
    - A classification system to identify critical systems and essential records
    - Mitigation strategies and safeguards to avoid disasters. Safeguards should include protective measures such as redundancy, fire suppression, uninterruptible power supply (UPS), surge protection, and environmental measures to protect sensitive equipment from dust, temperature, or humidity
    - Backups and offsite storage
    - Information Resource role in business continuity

- Contingency plans for different types of disruptions to Information Resource and systems availability
- Organizational responsibilities for implementing the disaster recovery plan
- Procedures for reporting incidents, implementing the disaster recovery plan, and escalating LTG's response to a disaster
- Multiple site storage of back-up documents
- Training, testing, and improvement
- Annual review and revision

5 GUIDELINES

5.1 Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Head.

5.2 Plan Documentation Storage

Copies of this Plan, Digital and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued an access to the digital copy and a hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued an access to the digital copy and hard copy of this plan.
A master protected copy will be stored on specific resources established for this purpose.

5.3 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site at the company's offices in BGC Taguig and PNB Makati This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (BRC Carmona) and the backup site (PNB Makati).

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Off-site data storage facility
Email	Not Applicable
Purchasing	Off-site data storage facility
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Off-site data storage facility
Human Resources	Off-site data storage facility
Web Site	Fully mirrored recovery site

5.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. 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:

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		
Electrical power failure	3	4	Redundant UPS array together with auto standby generator that is tested quarterly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	2	2	Two diversely routed link into building. WAN redundancy, data network resilience

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

5.5 Emergency Response

5.5.1 Alert, escalation and plan invocation

Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

5.5.2 Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the business, data center, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

5.5.3 Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

5.5.4 Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

5.5.5 Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

- _____
- _____
- _____

If not available try:

- _____
- _____

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated.

5.5.6 DR Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

5.5.7 Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

5.5.8 Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

5.5.9 Announcements/ Updates

For the latest information on the disaster and the organization's response, staff members can refer to the announcements and updates in the LTG messaging platform. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

5.5.10 Personnel and Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

5.6 Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, directors & officers liability, general liability, and business interruption insurance.

If insurance-related assistance is required following an emergency out of normal business hours, please contact: _____

Policy Name	Coverage Type	Coverage Period	Amount Of Coverage	Person Responsible For Coverage	Next Renewal Date

5.7 Financial and Legal Issues

5.7.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

5.7.2 Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

5.7.3 Legal Actions

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

5.8 DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

6 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Disaster Recovery Testing	IT Infra / ERT	IT Head / Unit Head	Information Security Office	Employee
Disaster Recovery Plan Execution	IT Infra/ ERT Administrative Services/ HR/	IT Head / Unit Head	Information Security Office	Employee

7 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image

- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~

LT Group, Inc.

LTG Backup and Restoration Policy

Table of Contents

1 OBJECTIVE

To maintain the integrity and availability of information and information processing facilities.

2 SCOPE

This policy applies to the production systems and project files of LT Group, Inc. (LTG), except the contents of the Network Temp Drives.

3 REFERENCE

ISO/IEC 27001:2013 Information Security Management System

4 POLICY STATEMENT

Regular backups shall be made for all production systems to protect against data loss in the event of a system fault.

Regular backups shall be made for project files to prevent data loss that would affect the timely completion of the project.

5 GUIDELINES

5.1 Production Systems

- IT Infra is responsible for performing regular backups for production systems of LTG.
- Regular backups shall be made for all production servers, with systems with frequent data updates being backed up more frequently (i.e. daily) and systems with less frequent data updates being backed up at longer intervals (i.e. weekly). For more information about Back up policies, refer to **Backup and Restoration Procedures and Guidelines**.
- Standard backup retention period of all production systems is three (3) months.
- A backup of a production server shall be performed before any major change to the system software or hardware can be undertaken (i.e. before an upgrade to the operating system or application software, before the migration of data to a larger disk array).
- Latest backups should be tested quarterly to ensure that the backup data is viable and can be successfully restored if necessary. For server images backups of virtual machines, restoration of the backed-up images on a non-production server shall be undertaken to test the integrity of the backup.
- Backup activities shall be logged, and backup media/files properly labeled.

5.2 Project Files

- Project managers are responsible for ensuring that project-related files are backed up regularly and properly.
- In the event that the project is completed, all project files should be turned over to IT Infra.

6 RACI

Process	R Responsible	A Accountable	C Consulted	I Informed
Backup of production systems	IT Infra (System and Storage Administrator)	IT Head	Information Security Office	Systems Owners
Maintenance of backup	IT Infra	IT Head	Information Security Office	Systems Owners
Backup of Project Files	Project Manager/IT Infra	Department Head	IT Infra / Information Security Office	-NA

7 SANCTION

Any violation to this policy is subject to the disciplinary sanctions as defined by the Human Resources Department. Below are the Classification / Gravity of Offenses and the Implementation of Corrective Action as described in the HR defined policies.

Implementation of Corrective Action

	1st Offense	2nd Offense	3rd Offense	4th Offense	5th Offense	6th Offense
Minor	Verbal Warning	Written Warning	Final Written Warning	1-5 Days Suspension	6-10 Days Suspension	Termination
Major	Written Warning	Final Written Warning	1-10 Days Suspension	Termination	NA	NA
Serious	1-10 Days Suspension	Termination	NA	NA	NA	NA
Grave	Termination	NA	NA	NA	NA	NA

Classification / Gravity of Offenses

Minor

- Has detrimental impact on business
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes very minimal indirect financial loss
- Has minimal impact for client, visitor, Company or Employee security but compromises the Company's ability to meet strict compliance with the security policies or
- Does not hurt any person physically but contributes to disorderliness in the workplace

Major

- Does not hurt any person physically but contributes to disorderliness in the workplace and / or
- Has some detrimental impact on business because of delay in operations or effect in productivity that is readily resolved by front-line Manager(s)
- Does not significantly losses the effectiveness of the team, but in some ways affects professionalism and Company image
- Causes more indirect financial loss or
- Has moderate impact on client, visitor, Company or Employee security and compromises the Company's ability to meet strict compliance with the security policy

Serious

- Causes delay in operations, productivity, and possible loss of opportunities
- Seriously compromises team effectiveness and relationships and therefore may result in team not being able to complete an assigned project or task, attain its specific objectives, or that may lead to dissatisfaction of the client or service provided
- Causes a considerable indirect financial loss
- Has high potential of compromising the security of clients, the Company, or other Employees or
- Poses real safety hazard and creates a possible occasion for injury

Grave

- Disrupts continuity of work and/or operations and breaks the public perception of the Company, which may have adverse effect on its relationship with its clients
- Causes any direct financial losses or substantial indirect financial loss to the Company
- It is a critical offense that has compromised the safety of client information, the integrity of client or Company's systems, and/or the security of other Employees or
- Results in physical harm

~ END OF DOCUMENT ~