LT GROUP, INC.

DATA PRIVACY POLICY

TABLE OF CONTENTS

1. ADMINISTRATIVE PROVISIONS

Distribution: All employees and contractors located in, or working for the LT Group, Inc. ("LTG"), including all of its subsidiaries (the "Group", collectively)

Issue Date: 11 February 2020

Effective Date: 11 February 2020

EXECUTIVE SUMMARY

To uphold the Law on Data Privacy, this Policy is established to ensure that all employees and contractors of the Group manage personal information (i) consistently with the requirements of this Policy; and (ii) in accordance with the Philippine Data Privacy Act of 2012 (DPA) and other applicable data privacy laws.

2. POLICY STATEMENT

2.1 All employees and contractors/suppliers/service providers of the Group are responsible for ensuring compliance with this Policy.

2.2 The LTG Data Protection Officer (DPO) is responsible for:

2.2.1 Implementing practices, procedures and systems relating to the Group's functions or activities that:

2.2.1.1 Will ensure that LTG complies with applicable privacy laws and privacy principles; and

2.2.1.2 Will enable LTG to deal with enquiries or complaints from individuals about the LTG's compliance with applicable privacy laws and privacy principles.

2.2.2 Considering requests from individuals for access to, and correction of, personal information

2.2.3 Receiving complaints from individuals regarding an alleged breach/es of privacy by LTG.

2.2.4 Investigating and resolving complaints internally through mediation with the individual.

2.3 The Group provides a framework for processing personal data in compliance with local data privacy laws and professional standards, as well as their own internal policies.

2.4 This Policy is based on the following principles:

2.4.1 To protect personal data using appropriate physical, technical and organizational security measures;

2.4.2 To process, store and disclose personal data only for legitimate business purposes;

2.4.3 To contain terms in contracts with third party suppliers to help ensure that company data is managed according to the same standards LTG implements across the enterprise;

2.4.4 To give additional attention and care to sensitive personal data, and to respect local laws and customs;

2.4.5 To identify appropriate measures to maintain personal data as accurate, complete, current, adequate and reliable; and

2.4.6 Where applicable, to provide notice to individuals with whom LTG engages, advising them of the purpose for which the Group is processing their personal information.

3. DATA PROTECTION OFFICER

3.1 A Data Protection Officer (DPO) has been appointed to champion data protection initiatives and be primarily responsible for monitoring LTG's compliance to relevant privacy and protection requirements.

3.2 The DPO must have direct reporting responsibilities to LTG's Executive Committee.

3.3 The DPO, in disposition of his/her duties, must perform the following:

3.3.1 Inform and advise the Executive Committee with regard the complaints and/or the exercise by data subjects of their rights;

3.3.2 Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing;

3.3.3 Ensure proper data breach and security incident management by LTG, including the preparation and submission to the National Privacy Commission (NPC) of reports and other documentation concerning security incidents or data breaches within the prescribed period;

3.3.4 Inform and cultivate awareness on privacy and data protection within the Group, including all relevant laws, rules and regulations and issuances of the NPC;

3.3.5 Serve as the contact person of LTG vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns; and

3.3.6 Coordinate and seek advice of the NPC regarding matters concerning data privacy and security.

4. APPLICABLE PRIVACY LAW

4.1 The DPA is a 21st century law that should address 21st century crimes and concerns. It (1) protects the privacy of individuals while ensuring the free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure and destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection through the NPC.

5. COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

5.1 Collection of Personal Information

LTG employees must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of LTG's functions or activities. LTG employees may collect personal information only by lawful and fair means and not in an intrusive way.

Whenever LTG employees and contractors collect personal information about an individual, they must take reasonable steps to ensure that the individual is aware of the following:

5.1.1 The identity and contact details of LTG as the organization collecting and storing the information;

5.1.2 The fact that he or she is able to gain access to the information and seek correction;

5.1.3 The purposes for which the information is collected;

5.1.4 The intended recipients or organizations to which LTG usually discloses information of that kind;

5.1.5 The right to object, on grounds relating to his or her particular situation, at any time to subsequent processing or changes to information supplied;

5.1.6 The right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from LTG's filing system;

5.1.7 The fact that he or she may make a privacy complaint and how LTG will deal with it;

5.1.8 Any law that requires the particular information to be collected; and

5.1.9 The main consequences (if any) for the individual if all or part of the information is not provided; and

5.1.10 The period of retention of information after processing.

Where it is reasonable and practical to do so, LTG employees will collect personal information about an individual only from that individual. If, however, this information is collected from a person other than the individual, LTG employees must act reasonably to ensure that the individual is or has been made aware of the matters listed above.

For a more detailed discussion, refer to Annex 01 xxx-xxx-xxx-001 Privacy Notice for Websites

5.2 Collection of Sensitive Personal Information

5.2.1 Sensitive Personal Information is information or an opinion which:

5.2.1.1 Concerns an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;

5.2.1.2 Concerns an individual's health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such individual, including the disposal of such proceedings or the sentence of any court in such proceedings;

5.2.1.3 Is issued by the government peculiar to an individual including, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

5.2.1.4 Is specifically established by an executive order or an act of Congress to be kept classified.

5.2.2 LTG employees must only collect sensitive information:

5.2.2.1 Where the information is reasonably necessary for one or more of the Group's functions or activities and with the individual's consent; or

5.2.2.2 If the collection is required by law.

5.3 Receiving Unsolicited Personal Information

Where LTG employees receive unsolicited personal information about an individual, they must determine, within a reasonable time, whether they could have collected the information in accordance with sections 5.1 and 5.2 above. If done accordingly, this Policy shall apply to the processing of such information.

Otherwise, the information must, as soon as practicable, and only if lawful and reasonable, be destroyed.

5.4 Collection of Personal Information for Research

LTG employees may also collect personal information for research about an individual from a party other than the individual concerned if:

5.4.1 The personal data is publicly available; or

5.4.2 There is consent from the data subject for purpose of research.

Provided, that adequate safeguards are in place and no decision directly affecting the data subject shall be made on the basis of the data collected or processed.

5.5 Use and Disclosure of Personal Information

As a general rule, LTG employees must not use or disclose personal information about an individual other than for its primary purpose of collection, unless:

5.5.1 The individual has consented to the use of or disclosure thereof; or

5.5.2 The individual would reasonably expect LTG to use or disclose non-sensitive information for a secondary purpose and the secondary purpose is related to the primary purpose; or

5.5.3 LTG has reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses such personal information as a necessary part of its investigation of the matter or to report its concerns to relevant persons or authorities; or

5.5.4 The use or disclosure is required or authorized by or under the law, rule or regulation; or

5.5.5 LTG reasonably believes that the use or disclosure is reasonably necessary for a specified purpose by or on behalf of an enforcement or other body; or

5.5.6 LTG reasonably believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety or the life or health of an individual; or

5.5.7 LTG must only use or disclose personal information in a manner consistent with any privacy notice provided to an individual.

5.6 Use and Disclosure of Government Related Identifiers

LTG employees must not use and/or disclose government related identifiers (e.g., social security numbers, previous or current health records, licenses or its

denials, suspension or revocation, and tax returns) unless such use or disclosure is reasonably necessary for LTG to verify the identity of the individual for the purpose of its activities, or alternatively, such use or disclosure is required or authorized under the law, rule or regulation.

6. DIRECT MARKETING

6.1 Use of personal information for direct marketing purposes is permitted where:

6.1.1 The information has been collected from someone other than the individual and LTG has obtained the individual's consent, or

6.1.2 When it is impractical for LTG to obtain the individual's consent before the use of the personal information, use thereof for direct marketing is permitted only when the individual has consented to the use of or disclosure of the information for that purpose.

6.2 When contacting individuals for direct marketing in whatever form, the following conditions must be followed:

6.2.1 LTG provides a simple means by which the individual may easily request not to receive direct marketing communications from LTG;

6.2.2 In each direct marketing communication with the individual, LTG draws to the individual's attention, or prominently displays a notice, that he or she may express a wish to "unsubscribe" or not to receive any further direct marketing communications;

6.2.3 The individual has not made a request to LTG not to receive direct marketing communications; and

6.2.4 LTG will not charge the individual for giving effect to a request not to receive direct marketing communications.

7. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

7.1 As a general rule, the LTG DPO will, on request by an individual, provide him or her with access to their personal information within a reasonable time after such request is made and will consider a request from the individual for correction of that information.

7.2 The LTG DPO cannot impose a charge upon the individual to cover the cost of locating, retrieving, reviewing and copying of any material requested by said individual.

7.3 The LTG DPO may however choose not to provide an individual with access to such information in cases where:

7.3.1 LTG reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;

7.3.2 Providing access would have an unreasonable impact on the privacy and affairs of other individuals;

7.3.3 The request for access is frivolous or vexatious or the information requested is trivial;

7.3.4 The information relates to anticipated or existing legal proceedings and would not be discoverable in those proceedings;

7.3.5 Providing access would reveal the intentions of LTG in relation to negotiations with the individual in such a way as to prejudice those negotiations;

7.3.6 Providing access would be unlawful;

7.3.7 Denying access is authorized under law, rule or regulation, or a court/tribunal order;

7.3.8 Providing access might prejudice an investigation of possible unlawful activity or affect security, defense or international relations;

7.3.9 Providing access might prejudice activities which are carried out by LTG on behalf of an enforcement or legal body; or

7.4 When an individual has been refused access to his/her personal information which LTG holds about said individual; or when refused of the request to correct his/her personal information, the LTG DPO will give the individual a written notice that sets out:

7.4.1 The reasons for the refusal, where it is reasonable to do so; and

7.4.2 The way in which the individual may make a complaint about such refusal.

For the templates used for accessing and correcting their information, refer to:

- *Annex 02 xxx-xxx-xxx-002 Access Request Form*
- *Annex 03 xxx-xxx-xxx-003 Request for Correction or Erasure Form*

8. MAINTAINING DATA QUALITY

LTG employees will take reasonable steps to make sure that the personal information they collect, use or disclose is accurate, complete, up to date and not misleading.

9. STORAGE AND TRANSMISSION

9.1 LTG shall implement approved security measures to all personal information stored onsite.

9.2 Access to stored personal information should be limited only to authorized and appropriate LTG employees.

9.3 LTG allows outside transmission of information to the effect that encryption is employed to personal information identified as sensitive.

10. RETENTION

10.1 Personal data shall be retained only for the duration necessary to fulfill the identified lawful business purpose. Retention of personal data of the data subjects shall only be necessary under the following circumstances:

10.1.1 For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated; or

10.1.2 The establishment, exercise or defense of legal claims; or

10.1.3 For legitimate business purposes, which must be consistent with standards followed by the industry; or

10.1.4 In some specific cases, as prescribed by law.

10.2 The Group shall develop guidelines and procedures for the retention of personal data which should address minimum and maximum retention periods, and modes of storage.

10.3 For LTG, the retention period for personal information is 20 years after inactivity. All hard, system, soft and electronic copies will disposed appropriately following LTG's disposal and destruction policy. In cases where information is intended to be kept after the retention period, subsequent consent from the data subject must be obtained.

10.4 Personal data collected for other purposes may be processed for historical, statistical or scientific purposes, and in certain cases as laid down by law, may be stored for longer periods, provided that adequate safeguards are guaranteed by said laws authorizing their processing, or consent has been obtained to retain and use for such purposes.

10.5 Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

11. DISPOSAL AND DESTRUCTION

11.1 Guidelines and procedures shall be developed for the secure disposal and destruction of personal data to prevent any further processing, unauthorized access, or disclosure thereof to any other party or to the public which would prejudice the interests of the data subjects.

The guidelines and procedures must likewise address the disposal processes on each of the following types of storage, including but not limited to:

11.1.1 Files that contain personal data, whether such files are stored on paper, film, optical or magnetic media; and

11.1.2 computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life, especially storage media, provided that the procedure shall include the use of degaussers, erasers, and physical destruction devices, among others.

11.2 Upon the expiration of identified lawful business purposes or withdrawal of consent, LTG must take reasonable steps to securely destroy or permanently de-identify/anonymize personal information if it is no longer needed. Data may be pseudonymized/anonymized, as deemed appropriate, to prevent unique identification of an individual.

11.3 Disposal should be in a manner that the personal data should be unreadable (for paper) or irretrievable (for digital records).

12. MAINTAINING DATA SECURITY

12.1 LTG employees must take reasonable steps to protect personal information held by the Group to avoid any misuse, interference and loss thereof and to prevent any unauthorized access, modification or disclosure of the same.

12.2 The Group shall ensure that appropriate physical, technical and organizational security measures are implemented on personal information storage facilities.

12.3 LTG employees must not keep personal information longer than necessary and must take reasonable steps to securely destroy or permanently delete or de-identify personal information when no longer needed.

13. INQUIRIES AND COMPLAINTS

13.1 LTG should receive all inquiries and complaints related to the privacy of the data subject as well as entertain and institute an investigation in relation thereof.

13.2 Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the Group, including the data privacy and security policies implemented to ensure the protection of

their personal data. The data subjects may write to the DPO and briefly discuss the inquiry, together with their contact details, for reference.

For the templates used for inquiries and complaints, refer to Annex 04 xxx-xxx-xxx-004 Inquiry/Complaint Form.

14. DATA INCIDENT NOTIFICATION PROTOCOLS

14.1 Data incident notification protocols are established and maintained in order to deal with an incident (i.e. an inadvertent disclosure of data, lost or stolen data or improper movement of data across national borders) concerning any personal information.

For detailed discussion on the data incident and breach protocols, refer to Appendix 1 for the guidelines on Privacy Incident Severity on this Policy.

14.2 LTG employees must immediately notify the LTG DPO if they become aware of a data incident to enable the appropriate assessment, investigation and remediation measures which should be undertaken in a timely manner (including possible notification to the National Privacy Commission (NPC) and other relevant bodies). If the incident occurs or is discovered outside normal working hours, the LTG DPO must be notified as soon as practicable.

For templates used for notifying the incident for investigation, refer to Annex 06 xxx-xxx-xxx-006 Data Breach Incident Report Template.

14.3 The LTG DPO shall maintain communications with the Information Technology (IT) Team. Incidents identified by the IT Team which affects the Group must be reported to the affected DPO of the respective subsidiary.

14.4 The DPO shall notify the NPC and affected data subjects within seventy-two (72) hours upon discovery or upon a reasonable belief that a personal data breach has occurred. Notification must be made when all of the following circumstances are present:

14.4.1 There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;

14.4.2 The data is reasonably believed to have been acquired by an unauthorized person; and

14.4.3 The personal information controller believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.

For templates used to notifying the NPC for breaches, refer to Annex 07 xxx-xxx-xxx-007 Data Breach Notification to NPC. For notifying the affected data subjects, the LTG DPO may opt to send formal letter or email.

14.5 If there is doubt as to whether notification is indeed necessary, the following factors are to be considered:

14.5.1 The likelihood of harm or negative consequences on the affected data subjects;

14.5.2 How notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and

14.5.3 If the data involves:

14.5.3.1 Information that would likely affect national security, public safety, public order, or public health;

14.5.3.2 At least one hundred (100) individuals;

14.5.3.3 Information required by all applicable laws or rules to be confidential; or

14.5.3.4 The personal data of vulnerable groups.

14.5.4 All events must be recorded in an incident reporting template.

Refer to the following templates:

- *Annex 08 xxx-xxx-xxx-008 Data Breach Incident Summary Tracker*
- *Annex 09 xxx-xxx-xxx-009 Data Breach Incident Report*

14.5.5 Initial investigation should be performed as soon as possible or within 24 hours from the time the personal data breach was reasonably believed to have occurred. Delay may be allowed if the scope of the breach cannot be determined within the 24-hour period. However, the 72-hour period notification to the Commission must be religiously observed.

14.5.6 After notifying the NPC, steps shall be taken to notify the affected data subject. The Group's authorized representative shall notify the data subjects individually through a secure means of communication such as written or electronic mail.

14.5.7 The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of the data subjects.

15. PRIVACY IMPACT ASSESSMENTS

15.1 Privacy Impact Assessment (PIA) should be completed when there are events that significantly change in the privacy environment, consisting the significant events set forth as follows:

15.1.1 New processes or modification to the current process

15.1.2 New projects

15.1.3 Marketing initiatives

15.1.4 Changes in the IT System Infrastructure

15.2 For changes in the IT System Infrastructure, the following triggers, at a minimum, should be considered:

PIA TRIGGER	DESCRIPTION
Digitization of records	Converting paper-based records to electronic systems.
Anonymous to Non-Anonymous	Operations performed on existing personal information database changes anonymous information into Sensitive Personal Information (SPI) or Personally Identifiable Information (PII).
Significant System Management Changes	New uses of existing IT systems, including the application of new technologies, significantly changes how SPI or PII is managed in the system. *For example, when the company employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.*
Significant Merging	The company adopts or alters business processes so that databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated. *For example, when databases are merged to create one central source of information, such a link may aggregate data in ways which may create privacy concerns not previously an issue.*

New User Access Mechanism	User-authentication technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by users (including Third Party users).
External Sources	The company systematically incorporates into existing information systems, databases of personally identifiable information purchased or obtained from third parties or public sources. An exception to this trigger would be merely querying such a source on an ad hoc basis using existing technology.

For the templates used for documenting PIAs, refer to:

- *Annex 10 xxx-xxx-xxx-010 Privacy Impact Assessment Template*
- *Annex 11 xxx-xxx-xxx-011 PIA Tracker*

16. DATA PROTECTION CLAUSE IN LTG STANDARD CONTRACT TERMS

In light of LTG's obligations under applicable data privacy laws, LTG's Standard Contract Terms shall include Data Protection wording to cover instances where the engagement involves collecting and processing personal information which has been provided to LTG.

Please refer to Appendix 2 for the suggested wording for a LTG contracts with possible privacy concerns.

17. PRIVACY CONTRACT/AGREEMENT FOR A SUPPLIER CONTRACT

In light of LTG obligations under applicable data privacy laws, LTG must ensure that appropriate wording is included in a suppliers/service providers contract where a third party supplier will receive, or will have access to any personal information that LTG holds.

Please refer to the following templates:

- *Annex 12 xxx-xxx-xxx-012 Data Sharing Agreement with Third Parties Template*
- *Annex 13 xxx-xxx-xxx-013 Outsourcing Sub-contracting Agreement Template*

18. CONSENT

In light of LTG obligations under applicable data privacy law, LTG must ensure that appropriate wording is included in their consent form where LTG will receive, or have access to any personal information.

Please refer to Appendix 2 for the suggested wording a consent form.

19. EDUCATION AND AWARENESS

LTG's directors, officers and employees must have access to all applicable Data Privacy policies, procedures, guidelines, incident reporting and Privacy Impact Assessment. Classroom training or E-learning must be developed for this purpose. Prospectively, subsequent communication of any changes will also be released /communicated via email and/or SMS.

Training materials include the following:

- Salient features of the DP IRR;
- Local Policies/Guidelines on Data Privacy;
- Roles and Responsibilities of Heads of Business Units/Employees
- Data Privacy Incident Reporting;
- Breach Reporting
- Privacy Impact Assessment;
- Violations to the policy

For the materials to be used for data privacy education and awareness, refer to Annex 14 xxx-xxx-xxx-014 Data Privacy Awareness Training

20. COMPLIANCE MONITORING AND REPORTING

20.1 Non-compliance with this Policy may result in a breach thereof, of the Data Privacy Act of 2012 and other applicable laws.

20.2 The Group shall maintain the inventories of Personal Data Processing systems. *(Refer to Annex 15 xxx-xxx-xxx-015 Personal Data Processing Systems Inventory).* Significant changes in the Personal Information Processing Systems shall be updated to the NPC within two (2) months after the implementation of the change.

20.3 LTG shall perform regular review of its forms, contracts, policies and procedures pertaining to ensure compliance to Data Privacy.

20.4 LTG, as applicable, shall perform regular privacy compliance monitoring, internal assessments and security audits.

20.5 LTG shall renew its annual registration to the National Privacy Commission within two (2) months prior to the deadline of 8th of March of the year.

21. EXEMPTIONS

Any requests for exemptions to this Policy should be referred to the DPO. Written approval from the DPO should then be forwarded to the person requesting such exemption.

22. AMENDMENTS

This Policy will be reviewed at least every two (2) years from its issue date or earlier if deemed required by either of the DPO or the Compliance Offer for Privacy (COP). All policy changes should be drafted by the DPO and approved by LTG Senior Management.

APPENDIX 1 – PRIVACY INCIDENT SEVERITY

1. PRIVACY INCIDENT SEVERITY

The severity of privacy incidents is considered during the classification of a privacy incident and is determined by taking into consideration the following factors:

- Volume of records
- Sensitivity of records

The method described below explains how to determine the severity of a privacy incident. This severity will ultimately determine the process, tasks and activities which need to be concluded in order to address the incident, based on the privacy risk that it poses to the Group.

1.1. Volume of Records

This refers to the number of data subjects who may be affected by a privacy incident.

LTG Group has defined the following thresholds for volume of records:

Low	Less than 10 data subjects
Medium	Between 10 and 100 data subjects (inclusive)
High	Greater than 100 data subjects

1.2. Sensitivity of Records

The possibility that information, if leaked or otherwise misused, would cause damage or harm to the data subject. The following guideline has been adopted at the Group level to determine sensitivity of records:

Low	No special personal information categories are included. (Low potential to cause financial loss or physical harm or harm to dignity.)
Medium	No sensitive personal information categories are included. (There exists some potential (neither low nor high) to cause financial loss or physical harm or harm to dignity.)
High	Sensitive personal information categories are involved. (High potential to cause financial loss or physical harm or harm to dignity.)

1.3. Severity Matrix

Taking into consideration both the volume of records and the sensitivity of the records affected by an event or incident, the following matrix is used to determine the overall severity of the incident, with Severity 1 incidents being most serious, to Severity 3 incidents having the lowest rating:

Volume	High (>100)	Severity 1	Severity 1	Severity 1
	Medium (10-100)	Severity 3	Severity 2	Severity 1
	Low (<10)	Severity 3	Severity 2	Severity 1
		Low	Medium	High
		Sensitivity		

2. INCIDENT RESPONSE TEAMS

In order to successfully investigate, respond to, and remediate an identified privacy incident, a basic requirement is to establish a cross-functional, multi-disciplinary incident response team.

Based on the severity of an incident, different role players may need to be involved. The sections which follow provide an indication of the role players who would need to be involved in the various severity categories of incident, but the actual role players who will be involved will need to be determined based on the specific nature and circumstances of any incident.

2.1. Severity 1 Response Team

Severity 1 incidents have the highest severity rating and as such need to be addressed more critically and comprehensively than incidents of a lower rating. Consequently, a larger response team involving more role players may be required to address a severity 1 incident.

Table 1: Severity 1 Response Team - Role Players

Mandatory role players to be involved in response *(kindly check applicability with the company's organizational structure)*	**Optional role players (dependent on nature of incident)** *(kindly check applicability with the company's organizational structure)*
Privacy Office	MANCOM representative
Affected Operating Unit / Support Function	Security Team
MANCOM representative	Information Technology
Legal Team	
Risk Office	

Severity 1 incidents are typically of such a nature that a war-room (e.g. a dedicated meeting room / office space) would likely need to be established to act as a central point for investigation, response and resolution of such an incident. All members of the response team need to convene in the war-room to establish critical next steps for the incident response. The war-room is only concluded once the incident is resolved, or the immediate urgency for resolution has passed and a suitable plan has been established.

2.2. Severity 2 Response Team

Severity 2 incidents have a moderate severity rating, and should be treated as important. However, it may not be required that the same level of seniority of the Group staff be involved in the incident response, and these incidents may not require as large a team to resolve them.

Table 3: Severity 2 Response Team - Role Players

Mandatory role players to be involved in response *(kindly check applicability with the company's organizational structure)*	Optional role players (dependent on nature of incident) *(kindly check applicability with the company's organizational structure)*
Privacy Office	MANCOM representative
Affected Operating Unit / Support Function	Security Team
Legal Team	Information Technology
Risk Office	Internal Audit

2.3. Severity 3 Response Team

Severity 3 incidents have the lowest severity rating, and thus it may be possible to address these with a smaller response team.

Table 4: Severity 3 Response Team - Role Players

andatory role players to be involved in response *(kindly check applicability with the company's organizational structure)*	Optional role players (dependent on nature of incident) *(kindly check applicability with the company's organizational structure)*
Privacy Office	MANCOM representative
Affected Operating Unit / Support Function	Strategic Communications
	Legal Team
	Risk Office

andatory role players to be involved in response *(kindly check applicability with the company's organizational structure)*	Optional role players (dependent on nature of incident) *(kindly check applicability with the company's organizational structure)*
	Security Team
	Information Technology
	Internal Audit

APPENDIX 2 – SUGGESTED WORDING FOR LTG CONTRACT

When LTG obtains personal data from any Third Party:

"We will Process the Personal Data in accordance with applicable law and professional regulations including, but without limitation to, the Data Privacy Act of 2012. We will require any service provider that processes personal data on our behalf to adhere to such requirements. You warrant that you have the authority to provide the Personal Data to us in connection with the performance of the Services and that the Personal Data provided to us has been, or can be processed in accordance with applicable law."

APPENDIX 3 – SUGGESTED WORDING FOR LTG CONSENT FORM

"To the extent necessary to provide the services to you and to your employer, you hereby authorize LTG to (1) obtain personal information from you, or from your employer, and (2) retain adequate documentation of the file in line with applicable laws and professional standards 20 years after the termination of the Services."

Alternatively, LTG may opt to use a form to fully disclose to the data subjects the purpose, usage, collection, sharing, retention and disposal of personal information and obtain consent for such processing. Refer to Annex 16 xxx-xxx-xxx-016 Consent Form Template.

APPENDIX 4 - DEFINITIONS

The table below defines the terms and definitions used in this policy.

TERM		DEFINITION
Access	-	Refers to an individual's right to see and know about his or her own personal information that an organization holds.
Collection	-	An organization collects personal information if it gathers, acquires or obtains information from any source, by any means, in circumstances where the individual is identified or is reasonably identifiable. It includes information that: ● is publicly available information about an identifiable individual that an organization comes across; ● information the organization receives directly from the individual; and ● Information about an individual an organization receives from somebody else.
Direct Marketing	-	Includes activities that promote the sale or purchase of products or services or promote charitable fundraising where the individual is approached directly. It includes in-person approaches to people's houses and approaches by mail, e-mail, facsimile and phone. It includes individually targeted approaches by these means where people are encouraged to buy services at a distance (for example to buy by phone, mail or website) or to visit retail and service outlets or to donate to a cause by one of these means.
Personal Information	-	Refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information, would directly and certainly identify an individual.
Primary Purpose	-	The primary purpose is the dominant or fundamental reason for information being collected in a particular transaction. There can only be one primary purpose of collection for a particular transaction. When an individual gives (and an organization collects) personal information, the individual and the organization almost always do so for a particular purpose, for example, to buy or sell a

particular product or to receive a service. This is the primary purpose of collection, even if the organization has some additional purposes in mind. These additional purposes will always be secondary purposes for that transaction, even if the organization tells the person about them, and even if the organization obtains the individual's consent to use or disclose the information for those additional purposes.

Reasonable - Generally speaking, they relate to decisions or steps to be taken by organizations in particular circumstances (for example, when collecting, correcting or using and disclosing information) or to expectations of individuals in those circumstances.

Determining what is reasonable involves considering the factual circumstances in which a person or organization is acting rather than the individual's or organization's view of what is reasonable or unreasonable.

Related Purpose - Includes all purposes directly related as well as certain additional ones. Related purposes must have some connection to, and must arise in the context of, the primary purpose.

Uses or disclosures for a related purpose would include uses or disclosures:

- giving a person information closely associated with a particular product or service a person receives from an organization; or
- notifying a person who has received a service or product from an organization in the past of a business change of address.

Required by Law - Refers to circumstances where a law (other than the Data Privacy Act of 2012) requires an organization to collect, use or disclose or deny access to, personal information. In certain instances, failing to comply with such a legal requirement may be an offense. Such a law may specifically require an organization to collect, use, disclose or deny access. It may also be a law that gives another body, such as a government agency, a general information gathering power that includes the power to require an organization to disclose information to it.

Sensitive Personal Information - Refers to personal information:

- about an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;

- about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of nay court in such proceedings;

- issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or it denials, suspension or revocation and tax returns; or

- specifically established by an executive order or an act of Congress to be kept classified.

Use of personal information relates to the handling of the personal information within the organization. Examples of uses of information are:

- adding information to a database;
- forming an opinion based on information collected and noting it on a file; and
- including information in a publication.

Vulnerable groups - Pertains to group of individuals that are susceptible to be harmed. This includes:

- children or minors;
- person with disability;
- senior citizen; and
- pregnant women.