MEDIA CONTACT
The offshore company

INFORMATION SYSTEM SECURITY POLICY

Revision History	
Last updated	December 2020
Modify by	

GROUPE MEDIA CONTACT SA
Avenue Dorothée LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

+229 **95 17 00 16**
contact@groupmediacontact.com

RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

Table des matières

I. DATA PROTECTION POLICY

Revision History	
Last updated	December 2020

GROUPE MEDIA CONTACT SA
Avenue Dorothée LIMA, rue 11010
Gbegamey Place Bulgarie
Immeuble Christophe, Cotonou Bénin
02 BP 8072 Cotonou

+229 **95 17 00 16**
contact@groupmediacontact.com

RCCM N° : RB/COT/13B 10291
IFU N° : 3201300930112

1. Data protection Principles

Group Media Contact is committed to processing data following its responsibilities under the data privacy laws. The privacy laws fundamentally require that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner concerning individuals.

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) Adequate, relevant and limited to what is necessary concerning the purposes for which they are processed.

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General Provisions

a) This policy applies to all personal data processed by the Group Media

Contact.

b) The Responsible Person shall take responsibility for Group Media Contact 's ongoing compliance with this policy.

c) This policy shall be reviewed at least annually.

d) The Group Media Contact shall register with any office/commissioner/statutory body to comply with relevant laws as an organisation that processes personal data if required to do so by a service provider.

3. Lawful, Fair and Transparent Processing

a) To ensure its processing of data is lawful, fair and transparent, the Group Media Contact shall maintain a Register of Systems.

b) The Register of Systems shall be reviewed at least annually.

c) Individuals have the right to access their data and any such requests made to the Group Media Contact shall be dealt with promptly.

4. Lawful Purposes

a) All data processed by the Group Media Contact must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.

b) The Group Media Contact shall note the appropriate lawful basis in the Register of Systems.

c) Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d) Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be available and systems should be in place to ensure such revocation is reflected accurately in the Group Media Contact's systems.

e) Data minimization

f) The Group Media Contact shall ensure that personal data are

adequate, relevant and limited to what is necessary concerning the purposes for which they are processed.

5. Accuracy

a) The Group Media Contact shall take reasonable steps to ensure personal data is accurate.

b) Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

6. Archiving / Removal

a) To ensure that personal data is kept for no longer than necessary, the Group Media Contact shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b) The archiving policy shall consider what data should/must be retained, for how long, and why.

7. Security

c) The Group Media Contact shall ensure that personal data is stored securely using modern software that is kept up to date.

d) Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

e) When personal data is deleted this should be done safely such that the data is irrecoverable.

f) Appropriate back-up and disaster recovery solutions shall be in place.

8. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal

data, the Group Media Contact shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the relevant authorities.

II. INFRASTRUCTURE SECURITY

Revision History	
Last updated	December 2020

9. Policy Statement

There shall be no unauthorized access to either physical or electronic information within the custody of the Group Media Contact. Protection shall be afforded to:

a) Sensitive paper records

b) IT equipment used to access electronic data.

c) IT equipment used to access the Group Media Contact's private network.

The Group Media Contact will promote awareness of this policy among their user communities.

10. Purpose

a) To ensure compliance with the legal statute and other mandatory controls and with best practice as defined within the ISO27001 and ISO9001 security standard.

b) To ensure the continued protection of the personal and sensitive information that the Group Media Contact holds and uses, in particular any information that has been classified as PROTECT, RESTRICTED or CONFIDENTIAL.

c) To ensure that any protection is appropriate to the sensitivity of the information and the risks associated with the loss of integrity, availability or confidentiality for that information, while at the same time, ensuring that minimum mandatory standards are complied with.

11. Scope

The policy defines what paper and electronic information belonging to Group Media Contact should be protected and offers guidance on how much protection can be achieved. This policy also describes employee roles and the contribution staff make to the safe and secure use of information within the custody of the Group Media Contact.This policy should be applied whenever a user accesses Group Media Contact information or its partners

information equipment.

This policy applies to all locations where information within the custody of the Group Media Contact or information procession equipment is stored, including remote sites. This document applies to all Committees, Departments, Partners, Employees of the Group Media Contact, Employees of Subcontractors providing services to Group Media Contact, contractual third parties and agents of the Group Media Contact who use Group Media Contact provided IT facilities and equipment, or have access to, or custody of, Group Media Contact customer information.

All users must understand and adopt this policy and are responsible for ensuring the safety and security of the Group Media Contact's systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

12. Policy

Applying the Policy

a) Assessing the impact of the loss of security

b) Detailed guidance on assessing the severity of any loss of information security (confidentiality, the integrity of availability) is contained within the Data Classification and Access Policy.

Baseline Group Media Contact Security standards

Physical security

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not restricted to, the following

- Alarms fitted and activated outside working hours.
- Window and door locks.

- Window bars on lower floor levels.
- Access control mechanisms fitted to all accessible doors (where codes are utilised, they should be regularly changed and known only to those people authorised to access the area/building).
- CCTV cameras.
- Staffed reception area.
- Protection against damage - e.g., fire, flood, vandalism. Particular attention will be paid to data centres and telecommunications equipment rooms.

Baseline secure areas

Any building or rooms within the Group Media Contact that are not normally open to the public are deemed baseline secure areas as a minimum. All buildings and rooms within the Group Media Contact are deemed baseline secure areas at times when they are not open to the public. Within baseline secure areas, the following is applicable :

- Employees should display their ID-Photo and must challenge anyone not displaying appropriate Group Media Contact identity passes (PhotoID)
- Each department must ensure that doors and windows are properly secured.
- Identification and access tools/passes (e.g., badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/provided to anyone else.

Enhanced secure areas

The designation of an enhanced secure area will take into account the impact levels of any data being stored or processed within that area plus other risks including theft, loss or personal injury to persons in that area. Where an enhanced secure area is designated all visitors are required to sign in and out with arrival and departure times and are required to wear an identification badge.

Where an enhanced secure area contains key ICT infrastructure components a member of the Group Media Contact's Information Management team

must monitor all visitors. Detailed procedures for the protection of areas containing key ICT infrastructure components are described in the Group Media Contact's Procedure manual for all ICT employees. Keys to all enhanced secure areas housing key ICT infrastructure components will be held securely by Information Management.

Duplicate keys may be held securely by the Group Media Contact's Security Personnel service where appropriate for security inspection and in event of fire or emergency. Keys must not be stored near these secure areas.

Responding to security breaches for any secure area

Where it is necessary to contact emergency services any locally based security personnel, this will usually precede any other action. Any employee may contact emergency services or on-site security personnel without the need for further authorisation. Employees must not put themselves, their colleagues or customers at risk of physical harm or injury.Reporting security breaches for any secure area

Reporting of a security breach serves several purposes including recording, analysis and determination of a subsequent response and implementation of preventative measures. Group Media Contact employees unauthorised access, theft or loss or other threat to security within a secure area (either baseline secure area or enhanced secure area) must be reported to Line manager who must, in turn, advise Security Head. In addition to the requirements of this policy' local facilities will be maintained in compliance with the document (periodically updated). Any unauthorised access, theft or loss or other threat to security within a secure area will be reported to local management who must, in turn, advise the Facility Manager for the premises in question.

Threats to Information assets

Where a security breach involves a threat to Information Security, the incident must also be logged with the Service desk. The incident will then be progressed as per the 'Information Security Incident Management policy and procedure.

Security of paper-based information

Paper-based (or similar non-electronic) information must be assigned an owner and a classification as stated in the Data Classification and Access policy. Where a document is classified and marked as PROTECT or RESTRICTED or CONFIDENTIAL, information security controls to protect it must be put in place. The exact nature of the controls will be determined by:

- A risk assessment that will consider the probability of any threat and the nature and sensitivity of the document
- Any mandatory controls specified by law, by sector compliance requirements or by contractual obligations

Appropriate measures to protect documents may include :

- Filing cabinets that are locked with the keys stored away from the cabinet.
- Locked safes.
- Stored in a Secure Area protected by access controls, in addition to these controls, it states that information marked as PROTECT, RESTRICTED or CONFIDENTIAL must not be left unattended on a desk.

ICT equipment Security

All general computer equipment must be located in suitable physical locations that :

- Limit the risks from environmental hazards – e.g., heat, fire, smoke, water, dust and vibration.
- Limit the risk of theft – e.g., if necessary, items such as laptops should be physically attached to the desk.
- Allow workstations handling sensitive data to be positioned to eliminate the risk of the data being seen by unauthorised people. Desktop PCs should not have data stored on the local hard drive. Data should be stored on the network file servers where appropriate. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.
- Servers will not reside outside designated data centres, which in turn will be deemed 'enhanced secure areas' and protected

accordingly.

- All items of equipment must be recorded on an inventory. Procedures must exist to ensure the inventory is maintained and current.
- All ICT equipment must be security marked and have a unique asset number allocated to it that cross-references to inventory
- For portable computer devices please refer to the following policies:
    - Remote and mobile working – Acceptable Use Policy
    - Removable media – Acceptable Use Policy

Cabling Security

Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas.

Equipment Maintenance Information

Information Management (IM) must ensure that all ICT equipment is maintained following the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order. This process will:

- Manufacturer's instruction manuals must be retained
- Maintenance will be following the manufacturer's instructions
- Any recommended service intervals will be recorded and adhered to
- There will be a call-out process to obtain maintenance and support in the event of equipment failure
- Only competent and authorised Information Management (IM) employees or agents of IM will maintain the equipment.
- Service histories (records of remedial work) will be maintained.
- Any insurance requirements will be identified

- Records of faults and remedial actions will be maintained. Service histories will be used to support business decisions relating to the timely replacement of ageing equipment

Security of equipment off-site

The use of equipment off-site must be undertaken in compliance with the following policies :

- Remote and mobile working – acceptable use policy
- Removable media – acceptable use policy

Users must also be aware of their responsibilities concerning Data Protection and be conversant with the Data Protection Act and other relevant legislation.

Secure Disposal or Re-use of Equipment

- Where a computer or media device must be reused outside the team it was originally assigned to, all data on the equipment must be securely erased prior to re-assignment
- Where a computer or media device has reached the end of its useful life, all data on the equipment will be securely erased and then disposed of in an environmentally friendly manner.
- Where disposal relates to a removable media device, the Removable Media Policy must also be referred to.
- Where equipment is to be passed onto another organisation (e.g., returned under a leasing agreement) secure date removal will be undertaken prior to equipment transfer. Secure data erasure practices will be subject to periodic verification by an independent 3rd party.

Delivery and Receipt of Equipment into the Group Media Contact

- Deliveries of ICT must be signed for by an authorised individual using an auditable formal process. This process should confirm that the delivered items correspond fully to the list on the delivery note.
- Actual assets received must be recorded

- Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.
- Subsequent removal of equipment should be via a formal, auditable process.

13. Regular Audit

Information Security arrangements will be audited regularly to provide an independent appraisal and recommend security improvements where necessary

Part Three: Enforcement, Governance, Definitions And References

14. Policy enforcement

The interpretation and application of this policy concerning any alleged non-compliance will be undertaken as follows :

Non Compliance	Enforcement Group
Employees	HR
Contractor	Relationship Manager and HR
VIsitors/Guest	Guest Relevent Department and HR
Snier Management	HR

Breaches of this policy will be subject to Group Media Contact Contact disciplinary policy and procedures, contractual terms and conditions and civil and criminal law which are appropriate.

15. Policy Governance

The following table identifies who within Group Media Contact is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

Functions	Description	Stakeholder
Responsible	The person responsible for developing and implementing the policy.	Head of Information Management and Head of Asset Management
Accountable	The persons who has ultimate accountability and authority for the policy.	Senior Information Risk Officer
Consulted	The persons or groups to be consulted prior to final policy implementation or amendment.	Human Resources, Legal services
Informed	The persons or groups to be informed after policy implementation or amendment.	All Group Media Contact employees, Group Media Contact members, temporary staff and contractors, suppliers and partner organisations.

16. Review and Revision

This policy, will be reviewed as it is deemed appropriate, but no less frequently than every 12 months. The policy review will be undertaken by Heads of Information Management and Asset Management or their delegates.

III. IP NETWORK SECURITY POLICY

Revision History	
Last updated	December 2020

17. Policy Statement

Group Media provides a wide range of services to the MNO across African regions thereby require a secure IT infrastructure. Many of the computer systems supporting these services use the Wide Area Network (WAN) to transmit sensitive information such as critical transactions, personnel and subscriber records, and proprietary corporate data. The Group Media is committed to protecting the integrity, confidentiality, and availability of its information systems, the sensitive information these systems handle, and the privacy of subscribers' information, while providing for efficient and effective management of this information.

18. Definitions

Wide Area Network (WAN

For this policy, the WAN is defined to include all lines and devices used to terminate data communication services from a service provider. The WAN may also be referred to as the Provincial Data Network in various service provider agreements and other contracts signed with vendors. WAN devices may include hubs, routers, switches, wireless devices, or other devices. The Security Committee determines whether devices are classified as WAN or not. In this definition, personal computers, file servers, printers, or other Local Area Network (LAN) devices are not generally classified as part of the WAN. (See illustration on following page).

19. Corporate Network

For this policy, the Corporate Network includes the WAN, as defined above, as well as LANs including file servers, personal computers, printers, and other computing or data communications devices that are used by any department, office, agency, board, or commission within the Group Media. Any other connected organization is considered an External Entity requiring specific authorization to connect and access the Corporate Network and is required to abide by the WAN Security Policy and Standards, including any revisions, while connected. This definition of the Corporate Network is

intentionally broad in scope to provide clear Committee boundaries for those charged with its security. (See illustration on following page).

Additional terms used in the body of this policy are defined in the glossary

The figure bellow is an Illustration of WAN and Corporate Network

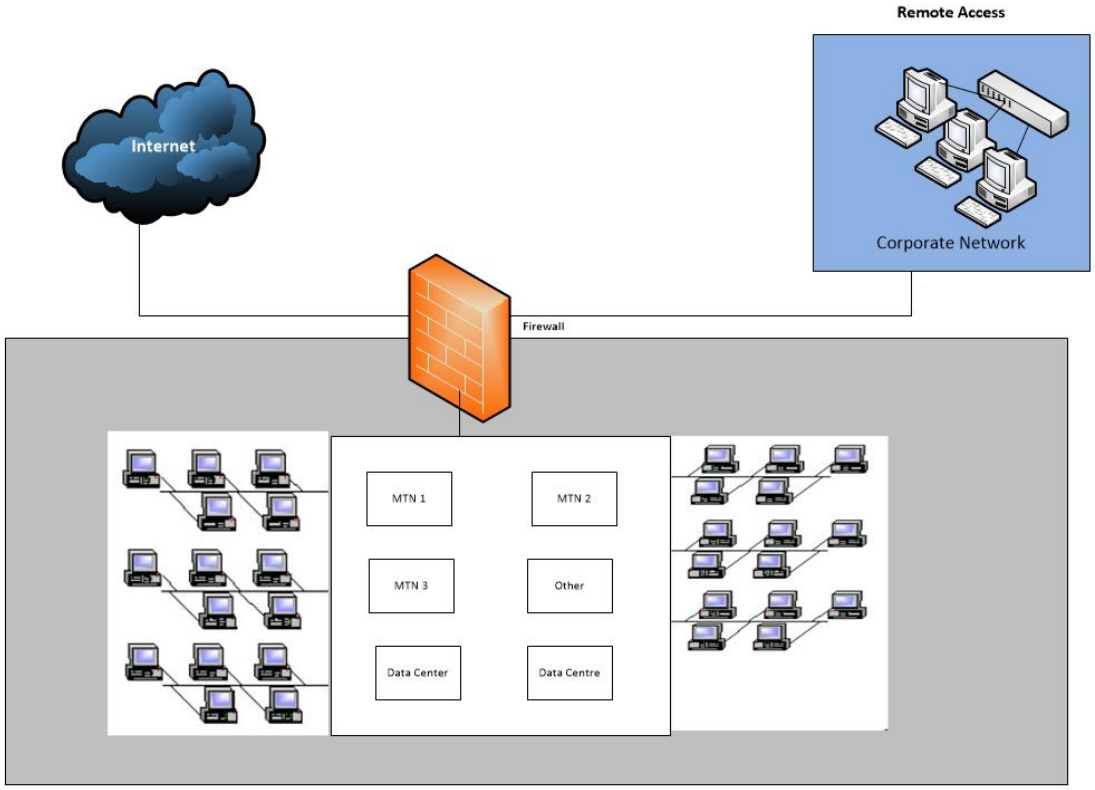

Figure 1: Conceptual Illustration of WAN Network, it is not intended as the true depiction of actual network

20. Policy Objectives

The objectives of this policy are to:

- Contribute to a secure WAN environment for all connected departments, offices, agencies, boards, and commissions.
- Provide a uniform security framework to secure the integrity, confidentiality, and availability of information and information systems, at the WAN level.
- Provide, in balance with operational requirements, legislative

requirements, and information sharing agreements, the minimum WAN security requirements.

- Raise awareness of information and information technology security needs for all users of the WAN by providing the security principles, requirements, and rules of use.
- Define the clear roles and responsibilities of all users of the WAN, particularly WAN security staff.
- Provide a foundation to develop and implement additional policies and standards as may be required to address specific security issues.

21. Application

This policy applies to all Corporate Network connected MNO, offices, agencies and Client Organizations, and other authenticated users in an authorized area of the WAN such as commercial organizations (External Entities). Any content covered by departmental policies also covered by or in conflict with any content in this policy is superseded by this policy. Additionally, this policy supersedes any prior policies related to WAN security such as the Firewall Gateway Policy.

22. Policy Directives

Policy directives are the minimum mandatory requirements that shall be met by MNO and External Entities.

Overall Network Security Guidelines

a) Access and use of Group Media Contact network must be always consistent with Group Media Contact network security policies and standards.

b) Network security control measures are to be consistently applied to all employees, computer systems and communications systems

c) Information must be protected based on confidentiality, value, and criticality; regardless of the media on which it is stored or the methods

by which it is moved.

d) Group Media Contact network security policies and standards will be reviewed on an annual basis, at a minimum, to ensure that they remain current. Security and Compliance Officer will review network security procedures and appropriate vendor guidelines on a semi-annual basis, at a minimum to ensure that the most current security measures are applied.

e) All Group Media Contact network components should be at least annually audited to make sure they remain in compliance with the Group Media Contact network security policies.

f) All employees must be provided with sufficient training and supporting reference materials to allow them to properly protect Group Media Contact network.

g) Security and Compliance Officer is responsible for identifying variances against generally accepted network security policies, and for promptly initiating corrective action.

h) All current Group Media Contact employees as well as well the new ones should be trained at least annually regarding the network security policies. Group Media Contact management must ensure that all employees read, understand, and sign the Group Media Contact network security policies.

i) Accountability and responsibility for following Group Media Contact network security policies on a day-to-day basis is every employee's duty.

j) Exceptions to network security policies and standards will only be made when the costs of implementing a standard exceed the security benefits or when the implementation will prohibit necessary Group Media Contact business activities.

k) Requests for changes to these statements contained in Network Security policies should be presented to and approved by the Group Media Contact management and Group Media Contact security consultant.

l) customer information (i.e., invoices) shall be treated with the highest level of sensitivity and any activities involving customer information shall be made in accordance with Group Media Contact security policies in

the same way as confidential internal information.

Identification/Authentication

a) All accounts, user IDs and devices in the Corporate Network shall be uniquely identifiable.

b) IT systems within the Corporate Network shall authenticate all users, applications and devices except for those designed specifically for anonymous access. These exceptions require the approval of the Security Committee.

Access Controls/Authorization

LAN

a) Enable Port Security to protect the switch from MAC address table exhaustion.

b) Enable DHCP Snooping to secure DHCP services from being spoofed.

c) Enable Dynamic ARP Inspection to limit address resolution protocol (ARP) use to valid traffic.

d) Enable IP Source Guard to prevent IP host address spoofing.

e) Enable the spanning-tree Bridge Protocol Data Unit (BPDU) Guard to protect network availability.

f) Enable IPv6 Router Advertisement Guard to protect devices from communication with an IPv6 router connected to user access ports.

g) Enable IPv6 DHCP Guard to protect devices from communication with an IPv6 DHCP server connected to user access ports.

WAN

a) All access points to the WAN shall be approved by the Security Committee.

b) All physical and logical connections to the WAN intended to provide access by individuals or groups shall be approved by the Security

Committee.

c) All WAN related address changes and configurations shall be approved by the Security Committee.

d) Any individual, office, or network connected to the Corporate Network shall require all employees to agree, through a signed or electronic agreement, to abide by the requirements outlined in the WAN Security Policy and Standards.

e) Requests for access to the WAN for an external entity shall be done through the Enterprise representative. The representative shall assume all responsibility for the entity requesting access.

f) Personnel who have access to sensitive information or are responsible for critical IT security functions such as network administrators and technical support staff require security screening.

23. Remote Access

a) Any remote access over untrusted networks shall use technology approved by the Security Committee to secure, monitor, and filter traffic.

b) All remote access to the WAN shall be authenticated, logged, and restricted to minimize the risk to WAN assets.

c) Infrastructure Service Management (ISM) of the Chief Information Office must ensure that remote access involving the WAN is monitored to protect the WAN security profile and confidentiality of sensitive information from unauthorized access and disclosure.

d) Any device which permits user-controlled access to the Corporate Network, such as a wireless modem, is not allowed except where permission is granted by the Security Committee.

e) All access to the Corporate Network shall occur through approved paths.

f) All users who use WAN resources remotely shall agree, through signed or electronic agreement, to abide by these requirements.

24. Firewalls

a) All communications between the Corporate Network and networks with different security profiles shall be protected by a network firewall approved by the Security Committee.

b) All firewalls and their configurations shall be provided and managed by the Security Committee except where the Security Committee approves Client Organizations to install and manage own firewall hosts.

25. Telecommunications Service Providers

a) All service providers contracting with Group Media such as suppliers of data communications or security services shall commit contractually to ensure that the WAN security profile is maintained.

b) All service providers contracting with Group Media Contact enterprises shall have access to the WAN Security Policy and Standards and agree to abide by them and ensure they are enforced within their organization.

c) Any exception to these directives shall be approved by the Security Committee and included as an addendum to the contract.

26. Contractors

a) All contracts or service agreements involving Corporate Network facilities, configuration, the management or any other application or server residing on the network shall include appropriate security clauses ensuring compliance with the WAN Security Policy and Standards.

b) All persons and organizations contracting with Group Media Contact (i.e., consultants, third-party sub-contractors, and casual and student employees) shall have access to the WAN Security Policy and Standards and agree to abide by them.

27. Physical and Environmental Security

a) An adequate environment (e.g., temperature, humidity, backup power supply) shall be provided to ensure optimum operation of the WAN and common infrastructure equipment as specified in the WAN documentation.

b) Physical controls shall be implemented to prevent unauthorized access to Corporate Network equipment including routers, switches, wiring racks, and network access servers.

c) The Security Committee shall have input into and final approval of all site design where WAN connectivity is being provided.

d) Access and use of Group Media Contact network must be always consistent with Group Media Contact network security policies and standards.

e) Network security control measures are to be consistently applied to all employees, computer systems and communications systems

f) Information must be protected based on confidentiality, value, and criticality; regardless of the media on which it is stored or the methods by which it is moved.

g) Group Media Contact network security policies and standards will be reviewed on an annual basis, at a minimum, to ensure that they remain current. Security and Compliance Officer will review network security procedures and appropriate vendor guidelines on a semi-annual basis, at a minimum to ensure that the most current security measures are applied.

h) All Group Media Contact network components should be at least annually audited to make sure they remain in compliance with the Group Media Contact network security policies.

i) All employees must be provided with sufficient training and supporting reference materials to allow them to properly protect Group Media Contact network.

j) Security and Compliance Officer is responsible for identifying variances against generally accepted network security policies, and for promptly

initiating corrective action.

k) All current Group Media Contact employees as well as well the new ones should be trained at least annually regarding the network security policies. Group Media Contact management must ensure that all employees read, understand, and sign the Group Media Contact network security policies.

l) Accountability and responsibility for following Group Media Contact network security policies on a day-to-day basis is every employee's duty.

m) Exceptions to network security policies and standards will only be made when the costs of implementing a standard exceed the security benefits or when the implementation will prohibit necessary Group Media Contact business activities.

n) Requests for changes to these statements contained in Network Security policies should be presented to and approved by the Group Media Contact management and Group Media Contact security consultant.

o) customer information (i.e., invoices) shall be treated with the highest level of sensitivity and any activities involving customer information shall be made in accordance with Group Media Contact security policies in the same way as confidential internal information.

28. Time Synchronization

All devices on the Corporate Network shall synchronize with a common central time source.

29. Revocation/Termination of WAN Privileges

The Security Committee shall take appropriate action, including termination of any connection or activity, at any time where the Security Committee feels the security of the WAN is or could be severely comprised. When circumstances permit, the Security Committee shall consult with the application owner before taking action. The Security Committee shall make a

full report of the actions taken and the reasons for such actions.

30. Change Control

a) All planned, scheduled changes to the WAN (power up, power down, configuration changes, and reset) shall be performed or authorized by the Security Committee.

b) A change control process shall be used to assess the security impact of major system upgrades and to support re-certification and accreditation. The change control process shall ensure that all system configurations and modifications are documented and retained in a secure environment for audit or future risk management considerations.

31. Security Risk Management Mechanisms and Planning

a) Security risk management based upon due diligence and due care shall be the primary basis to determine WAN security safeguards and residual risk and to maintain the accredited WAN security profile.

b) Re-assessments of the security profile shall take place if risk, system, or other relevant technological or organizational changes occur.

c) Before implementation, all new systems, as well as additions, deletions, or alterations to existing systems, shall be reviewed to ensure that the security profile of the Corporate Network is not compromised by the change.

d) The procurement and purchase of hardware and software must be reviewed by Network security management team. Development and users with elevated privileges must only use software that has been provided by a known and trusted person, supplier, or organization.

e) Group Media Contact communications networks will be designed

so that no single point of failure, such as a central switching or core router, could disrupt network service essential to the continuity of business. Any single points of failure that exist on networks given less priority should be documented.

f) System designers and developers should always follow the network security policies for system designs

g) Security will be a fundamental design criterion used in all data network designs. While it is understood that other factors can and will influence the final design whenever possible security considerations must be given the utmost consideration in any design exercise.

h) Every system design must have provisions for error recovery and an audit trail. All computer-assisted processes must involve human intervention prior to initiating any action that could result in service interruption or sustained service downtime.

i) Only one primary function shall be implemented per system component and in case of virtualization environment one function shall be implemented per virtual machine.

j) All new system security controls must be tested prior to implementation.

k) Software in development must be kept strictly separate from production software. This separation must be achieved via physically and logically separate computer systems and networks where possible.

l) Test functions should be performed separately from production and development environments. The results of testing will be fully documented and securely maintained for a reasonable period.

m) All changes to production systems must follow the change control policies.

n) There shall be no restriction on use of open-source software and tools, provided appropriate legal review of the source code licenses has been granted, use is consistent with that license, and the software is appropriately tested.

o) Group Media Contact employees must not possess or use code-

breaking software or hardware that allows illegal copying of proprietary software, discovery of passwords, or cryptanalysis of encrypted data.

p) The creation of any new network must be audited by Security and Compliance Officer and approved by the higher-level management.

q) The network architecture must be clearly documented.

r) Any changes to the existing architecture must follow the change control policies and procedures, and the relevant documentation must be updated immediately.

s) Network systems documentation (network diagrams, routing tables, IP addresses) are very sensitive information that will be restricted to authorized employees only.

t) All systems that store or process Group Media Contact or customers sensitive data will be protected using a firewall, or other approved network security devices, from public external networks.

u) Only authorized personnel will be allowed access to network equipment.

v) Different levels of access will be administered based on the job function, responsibility, and necessity of the employee's access.

32. Certification and Accreditation

IT system security certification and accreditation shall be performed on the Corporate Network (including all hardware and software that comprises the Corporate Network) throughout the planning, implementation, and operations life cycle.

33. Security Logs and Records

a) Appropriate logs shall be kept and reviewed as prescribed by the

Security LAN Access Layer

b) Enable Port Security to protect the switch from MAC address table exhaustion.

c) Enable DHCP Snooping to secure DHCP services from being spoofed.

d) Enable Dynamic ARP Inspection to limit address resolution protocol (ARP) use to valid traffic.

e) Enable IP Source Guard to prevent IP host address spoofing.

f) Enable the spanning-tree Bridge Protocol Data Unit (BPDU) Guard to protect network availability.

g) Enable IPv6 Router Advertisement Guard to protect devices from communication with an IPv6 router connected to user access ports.

h) Enable IPv6 DHCP Guard to protect devices from communication with an IPv6 DHCP server connected to user access ports.

i) All actual or suspected security incidents shall be recorded and reported to the Security Committee.

34. Incident Reporting and Investigation

a) All Corporate Network security incidents shall be reported and investigated immediately by the infrastructure or application owner, Client Security Officer or designate, the Security Committee, or others as appropriate. The Security Committee shall notify other Client Security Officers who may be affected.

b) The Security Committee may also conduct a self-instituted secondary investigation as requested by the infrastructure or application owner, Client Security Officer or designate to determine if there are additional security issues and the appropriate solutions.

35. Security Information/Documentation

a) WAN infrastructure shall be documented as required by the Security

Committee from time to time. The Security Committee shall be given access to this documentation on request to support WAN design security issues, disaster recovery operations, change control processes, diagnostic or hacker investigations, visual inspections, and security audits of the WAN infrastructure.

b) WAN security information and documentation including configuration, backups, and diagnostic information shall be password protected, physically stored under lock and key, and only released on the approval of the Security Committee. If located at a contractor site, the protective details and obligations shall be addressed in the contract.

c) Security information and documentation to be discarded, and which contains sensitive information such as passwords and IP addresses, shall be irretrievably destroyed securely by shredding, permanent electronic deletion, or by other means approved by the Security Committee.

36. Monitoring/Surveillance and Privacy

a) The Security Committee shall monitor the WAN for performance and security purposes.

b) Monitoring initiatives designed for the WAN shall operate within the legislated requirements for the protection of personal privacy.

c) Access or monitoring of LAN segments shall be in co-operation with network administrators.

d) No person shall operate sniffers or other monitoring devices on the Corporate Network without the prior knowledge of the Security Committee.

e) Corporate Network monitoring shall not involve reading data content unless it is required in the performance of duties.

f) Where there is reason to believe that an individual is engaging in inappropriate activity on the Corporate Network the content of individual files may be read. This would only happen in an approved investigation by appropriate authorities.

g) Any investigation of data content shall be conducted following

applicable human rights, and any applicable provincial and state legislation.

37. Security Training

a) The Security Committee shall provide training to all staff, Client Security Officers or designates, and others as necessary on WAN Security Policy and Standards including interpretation and application.

b) Client Organizations are responsible for the WAN Security training within their organization, and for any External Entities sponsored by them, required to ensure the performance of the security responsibilities outlined in the WAN Security Policy and Standards.

38. Accountabilities

General Managers (GM)

GM of each Client Organization is accountable for the overall security of all information within their jurisdiction.

Chief Information Officer

Chief Information Officer is additionally accountable for the strategic development and analysis of policy, standards, and processes for information security.

Security Policy Co-Ordinator

The Security Policy Coordinator is responsible for developing, monitoring, and proposing revisions to the WAN Security Policy and Standards in co-operation with WAN stakeholders.

Security Committee

The Security Committee is responsible for operational WAN security management and directs the implementation of the WAN Security Policy and Standards in co-operation with ISM, Client Security Officers or designates. The Security Committee evaluates and responds to all requests related to WAN access, services and security.

Client Security

A Client Security Officer or designate is the individual(s) assigned within each Client Organization to carry out security requirements and communications for their Client Organization and to work in co-operation with the Security Committee to ensure compliance with the WAN Security Policy and Standards.

Client Organization

A Client Organization is any department, office, agency, or enterprise in the Group Media connected to the Corporate Network and is required to abide by the WAN Security Policy and Standards.

External Entity

An External Entity is an organization having business with Group Media, sponsored by a Client Organization and authorized by the Security Committee, connected to the WAN. The External Entity shall agree to abide by the WAN Security Policy and Standards.

Managers And Delegated Staff

Managers and delegated staff, in addition to specific responsibilities cited above, shall have other specific responsibilities for such WAN aspects as availability, network upgrade and maintenance, security monitoring and incident reporting.

Organizations Hosting Wan Facilities

Organizations hosting WAN facilities such as routers, firewalls, wiring closets and other related components shall ensure that physical protection of WAN assets meets the WAN Security Policy and Standards.

39. Monitoring (of the WAN Security Policy)

General Manager

General Manager of each Client Organization is responsible for overall compliance with the WAN Security Policy and Standards.

Security Policy Co-Ordinator

The Security Policy Co-ordinator shall monitor WAN Security Policy implementation. This responsibility includes evaluating the suitability and

effectiveness of the policy and standards. The Security Policy Co-ordinator shall co-ordinate any necessary remedial action to address issues reported by the Security Committee in the annual WAN security report. The Security Policy Co-ordinator shall also ensure that the policy and standards are formally reviewed at least every two years.

Security Committee

The Security Committee is responsible for monitoring the operational security of the WAN ensuring that the established security profile is maintained, and that changing environments, potential threats, and evolving technology are addressed. The Security Committee shall report annually to the Security Policy Co-ordinator on the WAN security environment, identified issues and security incidents, and the effectiveness of the WAN Security Policy.

Infrastructure Service Management (ISM)

ISM shall monitor compliance with the WAN Security Policy and Standards for all IT systems within their jurisdiction. ISM shall notify the Security Committee and the Security Policy Coordinator to request a policy review.

Client Security Officer or Designate

The Client Security Officer or designate shall monitor compliance with the WAN Security Policy and standards for all IT systems within their jurisdiction. The Client Security Officer or designate shall notify the Security Committee and the Security Policy Coordinator to request a policy review.

40. Enquiries

All enquiries, requests, or comments should be forwarded to

CIO: Chief Information Officer

41. Glossary

Access Control

A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Accreditation
Approval by the responsible manager for the operation of an information technology system using a particular set of safeguards.

Authentication
The process of determining whether a person, workstation, system or procedure is eligible to access specific information, or to perform certain operations. Password validation, for example, is a form of authentication. Authentication may also be a measure meant to validate a transmission or message and the Committee of the originator.

Bastion Host
A server that is hardened against attack and can therefore be used as a critical component of network security. Firewalls and screening routers are examples of bastion hosts.

Certification
An examination by qualified personnel of an information technology system's implemented security safeguards against the system's security requirements.

Client Organization
See Accountabilities.

Confidentiality
The sensitivity of information or assets to unauthorized disclosure, recorded as highly confidential, confidential or protected, each of which implies a degree of injury should unauthorized disclosure occur.

Contractor
A third party involved in the direct management of the WAN or any part of it, quite often under a WAN management or data communications, service agreement. Contractors are required to abide by the WAN Security Policy and Standards.

Corporate Network
See Definitions

Due Care
Reasonable attention or caution which could be expected from an average person under the circumstances.

Due Diligence
A measure of prudence which could be expected from a reasonable and prudent individual having responsibility for some aspect of security risk

management. It carries with it a higher level of responsibility than "due care".

External Entity
See Accountabilities.

Firewall
A network security device positioned between networks with different security profiles that ensure all communications attempting to travel between the networks conform to the configured security profile

Integrity
The quality or condition of being accurate or complete.

Modem (Modular-Demodulator)
A device that converts digital signals used by computers and analogue signals used by the telephone or related telecommunication system which enables computers to communicate remotely. In the WAN Security Policy and Standards, a modem includes any telecommunications device such as a dial-up modem, cable modem, dedicated line modem, wireless device or digital subscriber line (DSL) device.

Monitor
The activity to ensure that information and assets, or the safeguards protecting them, are checked by security staff or electronic means with sufficient regularity to satisfy the WAN Policy and Standards.

Security Profile
A minimum acceptable level of security for the WAN established by the implementation of the WAN Security Policy and Standards.

Security Committee
See Accountabilities. All references to the Security Committee in this document means the Security Committee or a delegate appointed by the CIO from time to time.

Security Incident
An occurrence or situation that results in a compromise of sensitive information, assets, functionality, or a loss of availability or integrity.

Security Risk Management
The process by which resources are planned, organized, directed and controlled to ensure the risk of operating an IT system remains within acceptable bounds at optimal cost.

Service Provider

A third party involved in the direct management of the WAN or any part of it, quite often under a WAN management or data communications contract. Exceptions to the WAN Security Policy and Standards, if applicable, shall be documented in the service agreement.

Time Synchronization

Process of ensuring that all devices on the WAN have the same time to ensure the accuracy of records and logs.

Threat

Any potential event or act that could cause one or more of the following to occur : unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets, services, or injury to people. A threat may be deliberate or accidental.

Threat and Risk Assessment

An evaluation, based on the effectiveness of existing or proposed security safeguards, of the chance of vulnerabilities being exploited.

Untrusted Network

A network, such as the Internet, that has no basis for a user to have any confidence and assurance in its inherent security.

IV- SOFTWARE AND APPLICATION POLICY

Revision History	
Last updated	2020 ember

42. Policy Statement

Group Media Contact will ensure the acceptable use of software and applications by the employees, contractors and third parties.

43. Purpose

The purpose of this document is to state the software and application policy of Group Media Contact and its subsidiaries and associates. All existing GMC policies apply to the employees and stakeholder's conduct regarding software, especially (but not limited to) the following:

- Email Policy
- Third Party Policy
- IP Network Policy
- Data Protection Policy
- Data Classification Policy
- Internet Acceptable Usage Policy.
- Password Policy.

44. Scope

This document applies to all Employees, Departments, Partners, Employees of the GMC, contractual third parties and agents of the GMC who have access to Information Systems or information use for Group Media Contacts purposes.

45. Definition

This policy should be always applied on the GMC's computer equipment, Software, applications, or Information Systems

46. Risks

Group Media Contact recognizes that there are risks associated with users accessing and handling information to conduct official GMC business.

This policy aims to mitigate the following risks:

- Purchase of Software
- Use and Development of Application
- Use and installation of Software

Non-compliance with this policy could have a significant effect on the efficient operation of the GMC and may result in financial loss and an inability to provide necessary services to our customers.

47. Software Acquisition

All software acquired by GMC must be purchased through the normal procurement process by Procurement Department. Software may not be purchased through user corporate credit cards, petty cash, travel, or entertainment budgets.

Software acquisition channels are restricted to ensure that GMC has a complete record of all software that has been purchased for GMC computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

Under no circumstances should personal or unsolicited software (this includes screen savers, games, and wallpapers etc.) be loaded onto a GMC machine as there is a serious risk of introducing a virus.

48. Software Registration

The GMC uses software in all aspects of its business to support the work carried out by its employees. In all instances every piece of software is required to have a license and the GMC will not condone the use of any software that does not have a license.

Software must be registered in the name of GMC and the department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user.

The Information System (IS) maintains a register of all GMC software and will

keep a library of software licenses. The register must contain:

a) The title and publisher of the software.
b) The date and source of the software acquisition.
c) The location of each installation as well as the serial number of the hardware on which each copy of the software is installed.
d) The existence and location of back-up copies.
e) The software product's serial number.
f) Details and duration of support arrangements for software upgrades.

Software on Local Area Networks or multiple machines shall only be used in accordance with the license agreement.

Group Media Contact holds licenses for the use of a variety of software products on all GMC Information Systems and computer equipment. This software is owned by the software company and the copying of such software is an offence under the Copyright, Designs and Patents Act, unless authorized by the software manufacturer.

It is the responsibility of users to ensure that all the software on their computer equipment is licensed.

49. Applications

The application component of all information systems, that is developed in house or purchased from a third party, is designed using security engineering principles. These security engineering principles is applied to the entire lifecycle of the application element via a systems development life cycle methodology that includes security considerations at all stages of the life cycle.

Further, development of the application element of an information system includes the creation and execution of a security test and evaluation plan. The results of the tests and evaluation is documented and shared with key stakeholders. The application element of all information systems is logically separate user functionality from administrative functionality such that the interface for the one cannot be used to operate the other.

Procedure for handling applications

Applications will be developed according to set methodologies that enforce

security:

- Development processes should make use of documented and repeatable standards and processes.
- Security training should be provided for the development team.
- Quality management should be performed throughout the development process.
- Code should be developed in a dedicated and secured environment.
- Code should be stored in securely maintained repositories.

50. Software Installation

Software must only be installed by the IS, IT Helpdesk once the registration requirements have been met. Once installed, the original media will be kept in a safe storage area maintained by the IT Helpdesk. Software may not be used unless approved by the IS Head of Department, or their nominated representative.

Shareware, Freeware and Public Domain Software are bound by the same policies and procedures as all other software. No user may install any free or evaluation software onto the GMC's systems without prior approval from Information Services or equivalent department.

51. Application and Software Development

All software, systems and data development for the GMC is to be used only for the purposes of the GMC.

Software must not be changed or altered by any user unless there is a clear business need. All changes to software should be authorized before the change is implemented. A full procedure should be in place and should include, but not be limited to, the following steps:

1. Change requests affecting a software asset should be approved by the application/software asset's owner or by Changed Advisory Board (CAB)
2. All change requests should consider whether the change is likely to affect existing security arrangements and these should then be approved.

3. A record should be maintained of agreed authorization levels.
4. A record should also be maintained of all changes made to application/software.
5. Changes to software that must be made before the authorization can be granted should be controlled.

52. Personal Computer Equipment

Group Media Contact computers are GMC-owned assets and must be kept both software legal and virus free. Only software acquired through the procedures outlined above may be used on GMC machines.

Users are not permitted to bring software from home (or any other external source) and load it onto GMC computers. Generally, GMC-owned software cannot be taken home and loaded on a user's home computer if it also resides on a GMC computer. If a user needs to use software at home.

53. Software Misuse

GMC will ensure that Personal Firewalls are installed where appropriate. Users must not attempt to disable or reconfigure the Personal Firewall software.

It is the responsibility of all GMC staff to report any known software misuse to the appropriate IS department's Head of Department].

According to the Copyright, Designs and Patents Act, illegal reproduction of software is subject to civil damages and criminal penalties. Any Group Media Contact user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. GMC does not condone the illegal duplication of software and will not tolerate it.

54. Policy Compliance

If any user is found to have breached this policy, they may be subject to GMC's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offenders.

If you do not understand the implications of this policy or how it may apply to you, seek advice from Risk Management head.

55. Policy Governance

The Following table identifies who within Group Media is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

a) Responsible: the person(s) responsible for developing and implementing the policy.
b) Accountable: the person who has ultimate accountability and authority for the policy.
c) Consulted: the person(s) or groups to be consulted prior to final policy implementation or amendment.
d) Informed: the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Head of Information Management and Head of Development/Engineering
Accountable	Information Systems Steering Committee and Senior Information Risk Officer (SIRO)
Consulted	Information Steering group (ISG), Human Resources, Legal services
Informed	All Group Media Contact employees, Group Media members, temporary staff and contractors, suppliers, and partner organizations

56. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by IS.

57. Key Messages

- All software acquired must be purchased through the IS Procurement a department
- Under no circumstances should personal or unsolicited software be loaded onto a GMC machine.
- Every piece of software is required to have a license and the GMC will not condone the use of any software that does not have a license.
- Unauthorized changes to software must not be made.
- Users are not permitted to bring software from home (or any other external source) and load it onto GMC computers.
- Users must not attempt to disable or reconfigure the Personal Firewall software.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

V- DATA CLASSIFICATION AND ACCESS CONTROL POLICY

Revision History	
Last updated	2020 December

Domains : Asset Classification and Control

Communications and Operations Management

Physical and Environmental Security

Information Security Incident Management

58. Policy Statement

Information Services (IS) Responsibility

All IS employees who encounter sensitive Group Media Contact internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily Group Media Contact business activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, IS employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for IS for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

Addresses Major Risks

The IS data classification system, as defined in this document, is based on the concept of the need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect Group Media Contact information from unauthorized disclosure, use, modification, and deletion.

59. Applicable Information

This data classification policy applies to all electronic information for which IS is the custodian.

60. Procedures

Access Control

Each of the policy requirements outlined in this document are based on the concept of the need to know. If an IS employee is unclear how the requirements outlined in this policy should be applied to any circumstance, he or she must conservatively apply the need-to-know concept. That information must be disclosed only to those people who have a legitimate business need for the information.

System Access Controls

The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to Group Media Contact systems and their resources. Remote access shall be controlled through identification and authentication mechanisms.

Access Granting Decisions

Access to Group Media Contact sensitive information must be provided only after the written authorization of the Data Owner has been obtained. Access requests will be presented to the data owner using the Access Request template. Custodians of the involved information must refer all requests for access to the relevant Owners or their delegates. Special needs for other access privileges will be dealt with on a request-by-request basis. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by the relevant Data Owner following a system review schedule approved by the CTO/CIO Office and Operations Management or Risk Management.

61. Information Classification

Owners and Production Information

All electronic information managed by IS must have a designated Owner. Production information is information routinely used to accomplish business

objectives. Owners should be at the CTO/CIO level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the Group Media Contact management team who act as stewards, and who supervise how certain type of information are used and protected.

Restricted

This classification applies to the most sensitive business information that is intended for use strictly within Group Media Contact. Its unauthorized disclosure could seriously and adversely impact Group Media Contact, its customers, its business partners, and its suppliers.

Confidential

This classification applies to less-sensitive business information that is intended for use within Group Media Contact. Its unauthorized disclosure could adversely impact Group Media Contact or its customers, suppliers, business partners, or employees.

Public

This classification applies to information that has been approved by Group Media Contact management for release to the public. There is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

Owners and Access Decisions

Data Owners must make decisions about who will be permitted to gain access to information and the uses to which this information will be put. IS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

62. Object Reuse and Disposal

Storage media containing sensitive (i.e. restricted or confidential) information shall be empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the Director of IS Security.

63. Physical Security

Data Center Access

Access to the data centre must be physically restricted reasonably and appropriately.

Facility Access

All network equipment (routers, switches, etc.) and servers located in the corporate office and all facilities must be secured when no Group Media Contact personnel, or authorized contractors, are present. Physically secured is defined as locked in a location that denies access to unauthorized personnel.

Special Considerations for Restricted Information

If Restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must conform to data access control safeguards approved by IS and Corporate senior management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password-protected screen saver, or otherwise restricting access to the restricted information.

Data Encryption Software

Group Media Contact employees and vendors must not install encryption software to encrypt files or folders without the express written consent of IS Security.

64. Information Transfer

Transmission Over Networks

If Group Media Contact Restricted data is to be transmitted over any external communication network, it must be sent only in encrypted form. Such networks include electronic mail systems, the Internet, etc. All such transmissions must use a virtual public network or similar software as approved by the Information Security Team.

Transfer to Another Computer

Before any Restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

65. Software Security

Secure Storage of object and source code

Object and source code for system software shall be securely stored when not in use by the developer. Developers must not have access to modify program files that run in production. Changes made by developers must be implemented into production by Technical Operations. Unless access is routed through an application interface, no developer shall have more than reading access to production data. Further, any changes to production applications must follow the change management process.

Testing

Developers must at least perform unit testing. Final testing must be performed by the Quality Assurance team or the target user population.

Backups

Sensitive data shall be backed up regularly, and the backup media shall be stored in a secure environment.

66. Key Management

Protection of Keys

Public and private keys shall be protected against unauthorized modification and substitution.

Procedures

Procedures shall be in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

Safeguarding of Keys

Procedures shall be in place to safeguard all cryptographic material, including certificates. IS Security must be given copies of keys for safekeeping.

VI- PASSWORD POLICY

Revision History	
Last updated	2020 December

67. Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and protecting passwords at Group Media Contact.

68. Scope

This policy shall apply to all employees, contractors, and affiliates of GMC, and shall govern acceptable password use on all systems that connect to GMC network or access or store GMC data.

69. Policy

Password Creation

1. All user and admin passwords must be at least [8] characters in length. Longer passwords and passphrases are strongly encouraged.
2. Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
3. Passwords must be completely unique, and not used for any other system, application, or personal account.
4. Default installation passwords must be changed immediately after installation is complete.

Password Aging

1. User passwords must be changed every [3] months. Previously used passwords may not be reused.
2. System-level passwords must be changed on a quarterly basis.

Password Protection

1. Passwords must not be shared with anyone (including co-workers and supervisors) and must not be revealed or sent electronically.
2. Passwords shall not be written down or physically stored anywhere in the office.

3. User IDs and passwords must not be stored in an unencrypted format.
4. User IDs and passwords must not be scripted to enable automatic login.
5. "Remember Password" feature on websites and applications should not be used.
6. All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policy. If you believe your password may have been compromised, please **immediately** report the incident to GMC and change the password.

VII- THIRD-PARTY POLICY

Revision History	
Last updated	2020 December

70. Purpose

Our third-party policy helps the incumbent use their IT resources appropriately. The management of third-party access is essential to our everyday jobs. We want to ensure that our employees understand the limitations of using their corporate third-party software. Our goal is to protect confidential data from breaches, and safeguard our reputation and technological property and those of our partners.

71. Scope

This policy applies to all employees, vendors and partners who are assigned (or given access to) a corporate network and email.

72. Third-Party Access

Principal

The utilisation of third parties must be formally managed and controlled to ensure that all risks to Group Media Contact are quantified, accepted, and minimised where appropriate.

Practices

Third-Party Requirements

a) Third parties must agree to and sign a legally binding contract and, where relevant, a Service Level Agreement (SLA), before being granted access to Group Media Contact IT infrastructure.
b) Third Parties must sign a standard, approved Confidentiality Agreement
c) Where one is in force, Third Parties must agree to abide by the rules in the Code of Conduct applicable to the network, system or service being accessed. This may typically include a requirement not to connect elsewhere (including back to the Third Parties own corporate infrastructure) without prior authorisation.
d) Third Parties must provide full details of onward connectivity from systems accessing Group Media Contact infrastructure, especially if this includes connections to other Third Parties or public networks. Evidence of appropriate barriers or firewalls etc. must be provided.
e) Third Parties must co-operate with Group Media Contact during the

investigation of any incident and are expected to work with Group Media Contact in achieving ongoing compliance with the Group Media Contact IT Security Policies.

f) Dependent upon the nature of the service provided, Group Media Contact may seek a Right of Audit to ensure that controls are being followed and to investigate any incident. Third Parties are requested to co-operate with Group Media Contact in drawing up such an agreement.

g) All Third-Party staff, contractors and sub-contractors who are involved in access to Group Media Contact system or network infrastructure must be made aware of and be bound by these requirements.

h) Third-Party users must be individually identifiable and accountable for their actions, precluding the use of shared or team accounts. If shared accounts are unavoidable, the Third Party must give a firm commitment that it will be held wholly responsible for the actions of its staff, contractors, or agents.

i) Third Parties may be required to provide evidence (at a suitably high level) of their internal security management procedures and controls and their method of enforcement to demonstrate their ability to meet these requirements. This may include staff selection, training, and disciplinary procedures.

j) Third Parties must adequately protect access to resources which grant access to Group Media Contact infrastructure, at both a physical and a logical level. This may require locating equipment in a separately locked area with controls over its access.

k) Any dial-in access by Third Parties to Group Media Contact systems or networks, or the Third Parties own infrastructure if access to Group Media Contact resources is then made possible, must be subject to "Strong Authentication".

l) Access to Group Media Contact systems or networks across public network infrastructure such as the Internet or public packet-switched networks must similarly be strongly authenticated (and may not be granted).

m) Third Parties must hold any information provided about Group Media Contact, it's systems, networks, applications, personnel, procedures, and policies securely unless such information is already in the public domain. On termination of contract, all such information must be returned to Group Media Contact and/or all records securely destroyed.

n) Confidential information must not be sent by unencrypted email over

untrusted networks such as the Internet or by fax without appropriate controls to ensure it is received only by the intended recipient.

o) Where software, documents or other susceptible materials are being distributed, measures must be taken by the Third Party to prevent the introduction of viruses, trojan horses or other unauthorised modifications into the code.

p) Business data must not be captured for diagnostic or other purposes without prior authorization from Group Media Contact and strict internal controls over its use. Any data so captured must be securely destroyed at the earliest opportunity. A log must be kept of all such data capture activity recording the time, duration, purpose, authorisation, and individual carrying out the data capture. This log must be made available to Group Media Contact on request and as a matter of routine (e.g., at monthly service review meetings). NB. simple file deletion is often inadequate to remove all traces of data. A secure method of eradication must be employed.

Internal Requirements

a) All-access by Third Parties to Group Media Contact resources, data, or computerized business functions shall be subject to a formal contract or SLA which addresses security and control issues and defines responsibility for them

b) All accesses shall have a designated clear owner within Group Media Contact who is responsible and accountable for the contractual relationship and ensuring activities of the third party are monitored against the contract or SLA.

c) The contract or SLA must be drawn up and agreed prior to the provision of the access facility.

d) Before granting any third-party access, an Operational Risk Assessment (ORA) should be completed to understand the risks and what mitigating controls may be required. This should include assessing any systems involving personal data and their compliance with Data Protection legislation (POPI) where unauthorized access could lead to prosecution.

e) If access is as part of a collaborative computing session, be sure that the Third Party can only carry out authorised activities and view data they are authorised to see.

f) A detailed inventory must be maintained for all Third Party and Dial-In Access Points, this should include the following information:

- Owner of the entry point (who is responsible for the maintenance of this inventory)
- owner(s) of systems, applications and data accessed
- Description and classification of data accessed
- Reason for granting access
- Authorization/dispensation for access
- Level of access allowed, including any time of day or frequency constraints and any special privileges required or denied individuals allowed access methods of authentication
- Other security controls employed
- Third party name with contact(s) for review and escalation
- Details of risk assessment carried out (pointer to document)
- Date of last review and date for the next review.

g) Clear roles, responsibilities and procedures should be established by both parties for:
   - date of last review and date for the next review
   - liaison regarding business issues
   - liaison regarding technical issues
   - contract negotiation
   - service level agreement negotiation and review
   - service level reporting and monitoring
   - establishment, management, and technical support of the method of connection
   - administration of security controls and authentication systems
   - change management procedures
   - incident reporting and escalation
   - escalation of any service-related issues
   - escalation of any security-related issues (may require separate reporting lines).

h) Consideration should be given to enhancing application-level access controls when moving from in-house to Third Party service provision. It may be necessary to 'well-off' certain sensitive systems or applications from possible Third-Party access.

i) All users and especially Third-Party users must be restricted to authorized activities only.

j) As with internally managed systems, all unnecessary system diagnostic tools and utilities must be removed before putting a system or service live, or ways found to effectively control their use.

k) Where access is made over any network and particularly the Internet,

restrict addresses and protocols to only that necessary. Where possible, restrict third party access to authorized systems only by setting up a closed pipe or forced a path through the Group Media Contact infrastructure to the target systems or applications.

i) Audit trails of significant activity carried out by Third Parties must be produced, securely held for an appropriate period and reviewed at regular intervals.

j) The network or systems being accessed should have the ability to generate an alert in the event of unauthorized access attempts or unauthorized activity. It must be possible to shut down access in a rapid and controlled manner in the event of an attack or other exposure.

k) If the Third-Party is a company with multiple users authorized to access Group Media Contact systems, confirmation must be obtained that all users are informed and understand their obligations and responsibilities.

l) Monitoring for compliance with the requirements of the contract or SLA must take place regularly, at periods suitable for the sensitivity of the data or functions being accessed. E.g., access for software maintenance purposes must be audit trailed and reviewed as soon as possible after the event.

m) Group Media Contact must reserve the right to revoke the access of Third-Party personnel in the event of a suspected security breach.

n) All-access by Third Parties should either be strongly authenticated (where the third party is considered as trustworthy as a member of staff) or carefully firewalled (if such authentication and trust are not possible) or both. All Internet and Extranet firewalls must be formally approved following the Firewall Approval Process, prior to connection.

o) Access to Third Parties must be terminated when no longer required. The termination process must include the return or destruction of any confidential material by the third party and will be the responsibility of the business relationship owner within Group Media Contact.