Infrastructure Security

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

Table of Contents

1. 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.

2. 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.

3. 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.

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

Appropriate measures to protect documents may include :

a) Filing cabinets that are locked with the keys stored away from the cabinet.
b) Locked safes.
c) 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 :

a) Limit the risks from environmental hazards – e.g., heat, fire, smoke, water, dust and vibration.
b) Limit the risk of theft – e.g., if necessary, items such as laptops should be physically attached to the desk.
c) 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.
d) Servers will not reside outside designated data centres, which in turn will be deemed 'enhanced secure areas' and protected accordingly.

e) All items of equipment must be recorded on an inventory. Procedures must exist to ensure the inventory is maintained and current.
f) All ICT equipment must be security marked and have a unique asset number allocated to it that cross-references to inventory
g) 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:

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

a) Remote and mobile working – acceptable use policy
b) 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

a) 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
b) 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.
c) Where disposal relates to a removable media device, the Removable Media Policy must also be referred to.
d) 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

a) 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.
b) Actual assets received must be recorded
c) Loading areas and holding facilities should be adequately secured against unauthorised access and all access should be auditable.
d) Subsequent removal of equipment should be via a formal, auditable process.

5. 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

6. 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.

7. 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.

8. 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.