Software and Application Policy

Revision History	
Last updated	2020 December

Table of Contents

1. Policy Statement

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

2. 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.

3. 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.

4. Definition

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

5. 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.

6. 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.

7. Software Registration

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

Groupe Media Contact

www.groupmediacontact.com

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.

8. Applications

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

f 🐦 📷 ▶ *Groupe Media Contact*   🌐 *www.groupmediacontact.com*

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.

9. 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.

10. 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.

11. 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

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

f 🐦 📷 ▶ *Groupe Media Contact*   🌐 *www.groupmediacontact.com*

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.

12. 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.

13. 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.

14. 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.

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

f ⅴ ◎ ▶ *Groupe Media Contact*   www.groupmediacontact.com

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

15. 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.

16. 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.