MEDIA CONTACT
The offshore company

Third-Party Policy

Revision History	
Last updated	2020 December

Table of Contents

1. 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.

2. Scope

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

3. 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.

l) 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.