MEDIA CONTACT
The offshore company

Data Classification and Access Control Policy

Revision History	
Last updated	2020 December

Contents

Domains : Asset Classification and Control

Communications and Operations Management

Physical and Environmental Security

Information Security Incident Management

1. 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.

2. Applicable Information

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

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.