Technology term paper example

Business, Company

Security Policy Paper

Global Distribution Inc. Security Policy

I. Policy

A. Global Distribution Inc. strongly believes that it is in its best interest to protect the company’s information system infrastructure from internal and external threats by means of implementing a level of security that will address the vulnerabilities that will be described herewith. GDI’s information whether in a form of written, recorded or electronically produced will be protected from intentional and accidental disclosures, unauthorized use, modifications and destructions throughout its cycle. Protection includes the prescribed level of security in terms of the use, storage, transmission and process of information system resources, propriety software and equipment.

B. All policies and its encompassing processes are to be disseminated accordingly to all responsible individuals through proper documentation and ensure utmost compliance during implementation. This policy identifies particular procedures in documenting all activities. In addition documentations made in accordance to this policies and procedures should be retained for at least 10 years for electronic copies and at least 5 years for printed forms. The documents are to be frequently reviewed for their currency and appropriateness in which the time frame will be determined by each entity within GDI.

C. Each GDI department levels are encouraged to develop and contribute procedures, standard, and additional policies detailing the implementation guidelines that address additional functionality, and information system in each department. However, it is important that each contributed policies

should comply and aligned with this policy. Existing policies are to subject to evaluation for their currency and applicability to the new set of policies. In addition, prior management processes will also assessed and aligned with the new set of policies.

II. Scope

- The scope of this information security policy includes protecting confidentiality, availability and integrity of the information.
- The entire framework defined in this security policy applies to all departments, staff, executives and all stakeholders within GDI.
- The standard defined in this security policy applies to protect information pertaining to GDI operations, processes, staff and clients.

III. Risk Management

- Information networks and systems of GDI will be thoroughly evaluated on a scheduled basis in order to maintain the integrity of the company’s information system including documentation of vulnerabilities, threats and transmitted information. Evaluation procedures will examine all external and internal threats and vulnerabilities including electronic, non-electronic, natural and man-made information resources. Existing vulnerabilities that believed to be exposed to potential risks will be examined in each department to assess the level of mitigating solutions needed to address the problem. Lastly, the analysis will include evaluation of technological and information assets associated to the dissemination, transmission, collection, protection and storage of relevant data.
- The combination of vulnerabilities, asset values, and relation of risk to confidentiality, information availability, threats and integrity will be pointed

out and the frequency of risk occurrences will be analyzed at each entity level.

- The periodic assessment of the aforementioned areas of concerns, security measures will be implemented based on the impact that each threat may cause to the system.

III. Compliance

This information security applies to all staff, executives, associates, partners and affiliates of Global Distribution Inc. Failure to comply on the provisions set herewith will constitute applicable disciplinary action including dismissal. Furthermore, this security policy mandates that the officials and top executives of GDI are required to comply with the standards and provisions set forth by NISTIR 7788on Security Risk and standard model of network security measures. The possible disciplinary actions that may be instituted for, but are not limited to the following.

- Unauthorized disclosure of confidential information as stipulated in the company’s confidentiality statement.
- Unauthorized disclosure of access codes and or passwords
- Obtaining and using codes assigned to another person
- Attempting to obtain information using other person’s access passwords
- Installing and uninstalling of GDI’s proprietary and licensed software
- Intentional and malicious manipulation of GDI sensitive information such as client and proprietary information

All of these violations will constitute applicable disciplinary and legal consequences once the actions leading to such violations were proven to have occurred after a thorough investigation.

IV. Security Classification for Information

One of the most important aspects of security information is the identification of specific of information that requires protection. For GDI, the Sensitive, Public, Confidential and Private type of information are classified under this security policy. The criticality of such information may bring inevitable damages to the organization once being exposed to vulnerabilities and threats. It is the reason that proper and independent system infrastructure should be integrated to GDI and managing such should not be outsourced, otherwise the level of vulnerabilities and unauthorized access to critical information will become apparent. Control mechanism is needed to be able to manage GDI's information and systems.

V. Control

Access to critical information in the company will have a defined level of restrictions to hinder unauthorized access. Security measures will be addressed by this policy in order to maintain integrity of GDI's information and security.

- Identification - Each of the employees will be provided with unique username and password to their workstations. The access codes are to be created by information security control officer provided that he Human resources Department has confirmed that employment status of the employee including a description of position and responsibilities. This information will help the information control administrator to determine the level of access that will be provided to the employee and what sectors of information can be made available to the user.

- Authentication – verification of identity is significantly important as a first

security barrier to determine access level. The username and passwords issued to the individuals in the company are subjected to system authentication by means of cross-determining the personal detailed associated to the access code. The information control officer will make sure to obtain the updated user's information from HR to be encoded to the access administrator software. In case the user cannot remember his username, password or both, he will be requested to key-in details such as employee ID#, Social Security, Date of Birth and all other personal effects. The security encryption tool verify the information provided by the user and once verified will only allow limited access to information unless the user reported the problem to the administrator to request a new set of access codes.

- Cryptography – The information security system will use cryptographic software to transform the information user's readable information into data sets that would not render usability to the unauthorized user. This tool will provide GDI information security with improved authentication process, stronger intrusion defense and repels non-reputable access attempts. GDI's wireless infrastructure will also adopt the same security measure by implementing WPA/WPA2 protocols. Wired communication, information exchange, emails and data files transmission will use AES, X. 1035 and encryption software such as GnuPG and PGP for added protection.

VI. Process

GDI's information security requires every member of the company to practice due diligence and due care. Everyone is expected to demonstrate due care to ensure that everything necessary were done in accordance to

the provisions of the co0mpany rules and security guidelines stipulated in this information security policy. Sound business practices and principle expects that every action is aligned with prescribed legal ethical manner.

References

Http://ise. gov (n. d.). National Institute of Standards and Technology (NIST) information Security and Privacy Advisory Board. Retrieved June 26, 2013, from http://ise. gov/building-blocks-content/national-institute-standards-and-technology-nist-information-security-and

It. ubc. ca (n. d.). Security Policies - UBC Information Technology. Retrieved June 26, 2013, from http://www. it. ubc. ca/service_catalogue/information_security/security/security_policies. html

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2006). Information Security Standards and Global Business. Quality Integration IEEE, (1424407265), 2091-2095. Retrieved from http://www. ee. oulu. fi/mvg/files/pdf/pdf_1012. pdf

Sans. org (n. d.). SANS: Information Security Policy Templates. Retrieved June 26, 2013, from http://www. sans. org/security-resources/policies/#name