**Blue Team X**

**POLICY & PROCEDURES**

### **Information Classification and Sensitivity Policy**

### **Effective Date:** <Month Day, Year> **Rev.** 1

**Policy:** Blue Team provide the best products in electronics, movies, and other products at a cost saving service to customers worldwide. Blue Team will set the standard for protection of information from unauthorized access and comprmise or disclosure. Accordingly, Blue Team has adopted this information classification and sensitivity policy to provide a standard and guideline to protect the information assets.

**Purpose:** Blue Team associates will share in the responsibility for ensureing that company information assets receive an appropriate level of protection by observing this Information Classification policy:

* Blue Team Captain (BTC) or information ‘owners’ will be responsible for assigning classifications to information assets according to the standard information classification system presented below.
* The information category will be embedded in the information itself.
* All Blue Team members will be guided by the information category in their security related handling of Company information.

**Information Classification:**

|  |  |  |
| --- | --- | --- |
| **Information Category** | **Description** | **Examples** |
| Unclassified Public | Information is not confidential and can be made public without any implications for Blue Team. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital. | * Product brochures widely distributed * Information widely available in the public domain, including publicly available Blue Team web site areas. * Blue Team company reports as regulated by authorities. |
| Proprietary | Information is restricted to BTC approved internal access and protected form external access. Unauthorized access could influence Blue Team’s operational effectiveness, cause an important financial loss, provide a significat gain to competitor, or cause a major drop in customer confidence. Information integrity is vital. | * Passwords and information on Blue Team’s security procedures. * Know-how used to process client information. * Any and all Blue Team developed codes, whether used internally or externally. * Standard Operating Procedures used by Blue Team in conducting day to day operations. |
| Client Confidential Data | Information received from clients (includes customers) in any form for processing in production by Blue Team. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and access are vital. | * Client media. * Electronic transmissions from clients. * Product information generated for the client by Blue Team production activities as specified by the client. * Any product purchased by clients or activity during a normal transaction. |

|  |  |  |
| --- | --- | --- |
| Company Confidential  Datt | Information collected and used by Blue Team in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of Blue Team’s finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital. | * Salaries and other personnel data. * Accounting data and internal financial reports. * Confidential customer business data and confidential contracts. * Non disclosure agreements with clients/vendors. * Blue Team business plans. |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of** | **Author** | **Description of Changes** |
|  |  |  |  |
|  |  |  |  |