Data Security Policy

Date: **05 – 16– 2018**
Document Version: **1.0**

INTRODUCTION

The purpose of this policy is to outline essential roles and responsibilities within the Dynamic Software Solution for creating and maintaining an environment that safeguards data from threats to personal, professional and institutional interests and to establish a comprehensive data security program in compliance with applicable law. This policy is also designed to establish processes for ensuring the security and confidentiality of confidential information and to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information.

SCOPE

This policy applies Dynamic Software Solutions and staff, whether full- or part-time, paid or unpaid, temporary or permanent, as well as to all other members of the Software company. This policy applies to all information collected, stored or used by or on behalf of any operational unit, of Dynamic Software Solution. The more specific requirements shall take precedence over this policy to the extent there is any conflict.

DEFINITIONS

- **Information Resource**
  An Information Resource is a discrete body of information created, collected and stored in connection with the operation and management of the Dynamic Software Solution and used by members of the company having authorized access as a primary source. Information Resources include electronic databases as well as physical files. Information derived from an Information Resource by authorized users is not an Information Resource, although such information shall be subject to this policy.

- **Users**
  Users include virtually all members of the Dynamic Software Solutions to the extent they have authorized access to company Information Resources. But We not authorized to share the information with outside parties.

- **Computer System Security Requirements**
  Computer System Security Requirements shall mean a written set of technical standards and related procedures and protocols designed to protect against risks to the security and integrity of data that is processed, stored, transmitted, or disposed of through the use of Dynamic software solution information systems. The Computer System Security Requirements shall be set forth as an exhibit hereto. The Computer System Security Requirements establish minimum standards and may not reflect all the technical standards and protocols in effect at the Dynamic Software Solutions at any given time.

- **Specific Security Procedures**
  Specific Security Procedures are procedures by a project manager to address particular security needs of specific Information Resources sponsored within their area of responsibility, not otherwise addressed by this policy, or any Data Security Directives.

- **Data Security Working Group**
  The Data Security Working Group shall be chaired by the manager of Dynamic Software Solutions, and shall consist of those Data Security Officers as may be assigned to the group from time to time by the Data Security Committee.

DATA CLASSIFICATION

1. All information covered by this policy is to be classified among one of three categories, according to the level of security required. In descending order of sensitivity, these categories (or "security classifications") are "*Confidential*," "*Internal Use Only*," and "*Public*."

   - **Confidential*:*** information includes sensitive personal and institutional information, and must be given the highest level of protection against unauthorized access, modification or destruction. Unauthorized access to personal confidential information may result in a significant invasion of privacy, or may expose members of the your company company users to significant financial risk. Unauthorized access or modification to institutional confidential information may result in direct, materially negative impacts on the finances, operations, or reputation of your company.Examples of personal Confidential information include information protected under privacy laws, information concerning the pay and benefits of Company employees, personal identification information or medical / health information pertaining to members of the University community, and data collected in the course of research on human subjects. Institutional Confidential information may include Company financial and planning information, legally privileged information, invention disclosures and other information concerning pending patent applications. With or without any required security code, access code, personal identification number or password that would permit access to the resident's financial account and confidential information also includes "customer information," defined by the safeguards rule to mean any information containing personally identifiable information.

- **Internal Use Only** information includes information that is less sensitive than confidential information, but that, if exposed to unauthorized parties, may have an indirect or possible adverse impact on personal interests, or on the finances, operations, or reputation of your company. Examples of this type of data from an institutional perspective include internal memos meant for limited circulation, or draft documents subject to internal comment prior to public release.

- **Public information** is information that is generally available to the public, or that, if it were to become available to the public, would have no material adverse effect on individual members of your company internal users or upon the finances, operations, or reputation of your company.

2. All Information Resources, whether physical documents, electronic databases, or other collections of information, are to be assigned to a security classification level according to the most sensitive content.

3. Where practicable, all data is to be *explicitly classified*, such that Users of any particular data derived from an Information Resource are aware of its classification.

4. Any data which includes any personal information concerning a member of the University community (including any health information, financial information, academic evaluations, social security numbers or other personal identification information) shall be treated as Confidential. Other information is to be treated as Internal Use Only, unless such information appears in form accessible to the public (i.e., on a public website or a widely distributed publication) or is created for a public purpose.

POLICY AND SECURITY

1. The Manager of Computer Policy and Security shall, with input from the Data Security Working Group, identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of your company data. This identification and risk assessment shall include adopting means for detecting security system failures and monitoring the effectiveness of the Computer System Security Requirements.

2. The Manager shall, in conjunction with the Data Security Working Group, oversee the implementation of the Computer System Security Requirements and recommend changes to address risks, failures, or changes to business practices to the Data Security Committee.

3. The Manager shall work with other Dynamic Software Solutions system administrators to investigate any violation of this policy and any incident in which the security or integrity of

your company data may have been compromised, including taking the steps set forth below in response to a security breach.

4. The Manager shall work with other Dynamic Software Solutions system administrators to develop and review training materials to be used for employee training under this policy.

SECURITY RESPONSIBILITIES

1. It is the policy of the Dynamic Software Solutions that all confidential and other sensitive information be safe guarded from unauthorized access, use, modification or destruction. All members of the Dynamic Software Solutions share in the responsibility for protecting the confidentiality and security of data. This section of the policy assigns specific duties to each of the roles of Project Manager and Engineers, Sponsors, System Administrators, Users, and the other Technical Parties. However, it is likely that an individual will have responsibilities reflecting multiple roles with respect to certain information.

- Ensuring that all staff have the training and support necessary to protect data in accordance with this policy, all Data Security Directives, and any Specific Security Procedures applicable to such data.

- Designating and managing the efforts of one or more Sponsors and Data Security responsible persons for all Information Resources maintained in their area of responsibility.

- Approving access authorization of all Users of Information Resources maintained in their area of responsibility having a data classification of Confidential.

- Promulgating Specific Security Procedures.

- A Sponsor has primary responsibility for overseeing the collection, storage, use and security of a particular Information Resource. In cases where a Sponsor is not identified for any Information Resource, the project manager shall be deemed the Sponsor. A Sponsor is responsible for the following specific tasks associated with the security of the information:

  - Ensuring that the Information Resource is assigned a security classification and that such data is marked where appropriate.

- Identifying authorized Users of the Information Resource, whether by individual identification of by job title, and obtaining approval for such access from their company management.

- Proposing to their company management Security Procedures for the handling of data under their sponsorship, consistent with this policy and other applicable University policies and procedures.

- Users are responsible for complying with all security-related procedures pertaining to any Information Resource to which they have authorized access or any information derived therefrom that they possess. Specifically, a *User* is responsible for:

  - Becoming familiar with and complying with all relevant company policies, including, without limitation, this policy, and all Data Security Directives contemplated hereby, the policy on Professional Standards and other policies related to data protection, technology use and privacy rights.

  - Providing appropriate physical security for information technology equipment, storage media, and physical data. Such equipment and files shall not be left unattended without being locked or otherwise protected such that unauthorized Users cannot obtain physical access to the data or the device(s) storing the data.

  - Ensuring that Confidential or Internal Use Only information is not distributed or accessible to unauthorized persons. Users must not share their authorization passwords under any circumstances. Users must avail themselves of any security measures, such as encryption technology, security updates or patches, provided by Data Security Officers. Users must log off from all applications, computers and networks, and physically secure printed material, when not in use.

  - your company Confidential or Internal Use Only data, when removed from the campus or when accessed from off-campus, is subject to the same rules as would apply were the data on campus. Sponsors and Users will comply with this Policy and all relevant Data Security Directives irrespective of where the your company data might be located, including, for example, on home devices, mobile devices, on the Internet, or other third-party service providers.

  - When access to information is no longer required by a User, disposing of it in a manner to insure against unauthorized interception of any Confidential or Internal Use Only information. Generally, paper-based duplicate copies of confidential documents should be properly shredded, and electronic data taken from confidential databases should be destroyed.

- Immediately notifying his or her cognizant Data Security Officer of any incident that may cause a security breach or violation of this policy.