webdesignuk

Data Classification & Access Policy

Terminology:

Employee or member of staff: someone employed to work for the Business, whether as a fully employed person or as a contractor.

The Business: Web Design UK, or any of its other brand names.

1. Policy Statement

1.1 All Web Design UK employees who come into contact with sensitive Web Design UK internal information are expected to familiarise themselves with this data classification policy and to consistently use these same ideas in their daily Web Design UK business activities.

1.2 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, Web Design UK employees are expected to apply and extend these concepts to fit the needs of day-to-day operations.

1.3 This document provides a conceptual model for Web Design UK for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

1.4 Addresses Major Risks - The Web Design UK data classification system, as defined in this document, is based on the concept of 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.

1.5 This concept, when combined with the policies defined in this document, will protect Web Design UK's information from unauthorised disclosure, use, modification, and deletion.

1.6 Applicable Information - This data classification policy is applicable to all electronic information for which Web Design UK is the custodian.

2. Procedures

2.1 Access Control:

a) Need to Know - Each of the policy requirements set forth in this document are based on the concept of need to know. If a Web Design UK employee is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information.

b) System Access Controls - The proper controls shall be in place to authenticate the identity of users and to validate each user's authorisation before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorised access. Controls shall be in place to ensure that only personnel with the proper authorisation and a need to know are granted access to Web Design UK systems and their resources. Remote access shall be controlled through identification and authentication mechanisms.

c) Access Granting Decision - Access to Web Design UK sensitive information must be provided only after the written authorisation of the Data Owner has been obtained. 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 in accordance with a system review schedule

approved by the manager of Information Services.

d) Review of Access Rights – Employee access rights will be reviewed at commencement of employment, when an employee leaves and at 12 monthly intervals during employment.

2.2 Information Classification:

a) Owners and Production Information - All electronic information managed by Web Design UK must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners should be at the Owner level. 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 Web Design UK management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

b) **RESTRICTED** - This classification applies to the most sensitive business information that is intended for use strictly within Web Design UK. Its unauthorised disclosure could seriously and adversely impact Web Design UK, its customers, its business partners, and its suppliers.

c) **CONFIDENTIAL** - This classification applies to less-sensitive business information that is intended for use within Web Design UK. Its unauthorised disclosure could adversely impact Web Design UK or its customers, suppliers, business partners, or employees.

d) **PUBLIC** - This classification applies to information that has been approved by Web Design UK management for release to the public. By definition, there is no such thing as unauthorised disclosure of this information, and it may be disseminated without potential harm.

e) 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. Web Design UK must take steps to ensure that appropriate controls are utilised in the storage, handling, distribution, and regular usage of electronic information.

webdesignuk

3. Object Reuse and Disposal

Storage media containing sensitive (i.e. restricted or confidential) information shall be completely 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 manager of Web Design UK security.

4. Physical Security

4.1 Data Centre Access - Access to the data centre is physically restricted in a reasonable and appropriate manner.

4.2 Facility Access - All network equipment (routers, switches, etc.) and servers located in the corporate office and in all facilities must be secured when no Web Design UK personnel, or authorised contractors, are present. Physically secured is defined as locked in a location that denies access to unauthorised personnel.

5. Special Considerations for Restricted Information

5.1 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 Web Design UK.

5.2 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.

5.3 Data Encryption Software - Web Design UK employees and vendors must not install encryption software to encrypt files or folders without the express written consent of Web Design UK Security.

6. Information Transfer

6.1 Transmission Over Networks - If Web Design UK Restricted data is to be transmitted over any external communication network, it must be sent only in encrypted form.

6.2 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.

7. Software Security

7.1 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 actually run in production. Unless access is routed through an application interface, no developer shall have more than read access to production data. Further, any changes to production applications must follow the change management process.

7.2 Testing - Developers must perform any website changes testing on a separate domain to the client's main domain. Final testing must be performed by Web Design UK management and the client.

7.3 Actual software development will be carried out on a separate server.

7.4 Backups - Sensitive data shall be backed up regularly, and the backup media shall be stored in a secure environment.

7.5 Please also refer to our other policies available within the Client Area here https://webdesignuk.agency/client-area/# our-policies