



Reddan Security & Confidentiality Policy

1 PURPOSE

The purpose of this Confidentiality Policy ("Policy") is to outline Reddan Group PLC's standards regarding confidential information, including the obligations and responsibilities of associates, contractors, and any other persons working for or on behalf of Reddan Group PLC, to protect and maintain confidential information that is within Reddan Group PLC's possession, custody and control.

The policy is derived from our corporate values, ethical obligations, legal requirements, and standards of practice concerning the confidential information that we maintain for our customers and their clients

2 SCOPE

This policy applies to all Reddan Group PLC associates, contractors, and other persons working with confidential information that is within the possession, custody, or control of Reddan Group PLC. For purposes of this Policy, "confidential information" means all customer data, Company data, and application and systems software that is created, stored, accessed, and distributed, regardless of whether such information is in physical or electronic form.

3 POLICY STATEMENT

3.1 Governance

Overall responsibility for ensuring compliance with this Policy rests with the Chief Information Security Officer (CISO). All Company Custodians must comply with this Policy in connection with day-to-day use, collection, and processing confidential information in the ordinary course of Reddan Group PLC's business.

3.2 Management

Each manager is responsible for ensuring that Reddan Group PLC employees within such Company manager's area(s) of responsibility are complying with this Policy. Reddan Group PLC management is also responsible for making all external parties aware of any changes to our confidentiality policy.

3.3 Staff and Contractors

All Company Custodians are responsible for ensuring that appropriate steps are taken to protect Client confidential Information at all times. Company Custodians are encouraged to regularly review and consult this Policy to ensure their own practices are in accordance with this Policy as it concerns the collection, access, use, or disclosure of confidential information. Company Custodians are expected to report any issues, problems, questions and concerns about this Policy to the CISO. Company Custodians are encouraged to make suggestions to the CISO to help improve privacy and security procedures. In the event of any incident involving confidential information or privacy and data security, Company Custodians are expected to fully cooperate with such investigations.



3.4 Acknowledgement of Confidentiality

In order to promote compliance with this Policy, Reddan Group PLC requires that all Company Custodians be provided with a copy of this Policy. Reddan Group PLC management must also regularly refresh and remind Company Custodians of this Policy and the importance of maintaining the confidentiality of confidential information. As a condition of employment or affiliation with Reddan Group PLC, all new employees and contractors are required to read and sign a Confidentiality Acknowledgment or non-disclosure agreement, which specifies that such employee or contractor understands the importance of maintaining the confidentiality of confidential information and will fully comply with this Policy. Reddan Group PLC employees and Company Custodians are also required to maintain confidence over confidential information after their affiliation with Reddan Group PLC comes to an end.

3.5 Failure to Comply

Any failure by a Reddan Group PLC employee or Company Custodian to comply with this Policy may result in disciplinary action including, but not limited to, the termination of employment or affiliation with Company.

3.6 Collection of Confidential Information

The collection of confidential information by Reddan Group PLC is governed by applicable international, federal and state law. As a practical matter, the collection of confidential information should be limited to what is needed to fulfil a specific purpose identified to the client or other person from whom it is collected.

3.7 Accuracy of Confidential Information

All Company Custodians must take all reasonable steps to ensure the accuracy and completeness of any confidential information that such Company Custodians collect or record. Company Custodians must be diligent to protect against making any errors due to carelessness or other oversights.

3.8 Access, Use, Disclosure or Sharing of Confidential Information

Company Custodians are only authorized to access, use, disclose or share confidential information for legitimate business purposes and should be limited to those Company Custodians who have a “need to know” such information in order to perform their job functions and responsibilities.

3.9 Release of Information

Company Custodians are expected to comply with all Reddan Group PLC policies, procedures and guidelines for the release of confidential information. Company Custodians must also ensure that any release of confidential information, including personally identifiable information is done in accordance with applicable law.

3.10 Accessing or Sharing Confidential Information with Third Parties

Before confidential information that is within the possession, custody, or control of Reddan Group PLC is accessed by or shared with a contractor or other third-party organization, the third party must execute a Non-Disclosure Agreement (NDA) or information sharing agreement with Reddan Group PLC. Senior Company management must approve the form of all such agreements.



All Company Custodians are required to take all reasonable steps to ensure no unauthorized personnel or third parties are provided with access to records containing confidential information. In the event a third party requests access to confidential information, all of the following steps must be taken prior to granting access: (1) the third party must produce identification verifying their identity, (2) a Reddan Group PLC manager must confirm that the third party has signed a non-disclosure or information sharing agreement with Reddan Group PLC, (3) a Reddan Group PLC Manager must confirm that the applicable Reddan Group PLC management has approved the third party for access to confidential information, and (4) the third party's access to such confidential information is limited only to the information absolutely necessary for such third party to perform their job task or function.

The CISO must be consulted before any program is implemented in which confidential information will be transmitted outside the boundaries of the Reddan Group PLC system.

3.11 Security of Information

Reddan Group PLC is committed to maintaining the security of confidential information and other sensitive information and has implemented technical and organization security mechanisms to help ensure the security and availability of physical and digital records, computer, and network systems. All Company Custodians are expected to comply with Reddan Group PLC's security requirements and policies for use of such systems, including without limitation, Reddan Group PLC's Acceptable Use Policy.

3.12 Retention and Destruction of Confidential Information

Reddan Group PLC Records will be retained in accordance with Reddan Group PLC's Record Retention Policy and all legal, regulatory and accreditation requirements. It is the responsibility of each Company Custodian in possession of a Reddan Group PLC record to identify the applicable retention period for the particular record and to follow Reddan Group PLC guidelines and procedures for the secure destruction of those records when the applicable retention period has expired and the information is no longer necessary to retain.

3.13 Compliance Monitoring, Auditing & Consequences

Access, use, and disclosure of confidential information will be monitored by Reddan Group PLC. All suspected breaches of this Policy will be investigated by Reddan Group PLC management. Any actions taken as a result of such a breach will be determined by Reddan Group PLC management in consultation with representatives from Human Resources, Legal Services and/or other Reddan Group PLC stakeholders, depending upon the nature of the breach, circumstances, and parties involved. Each Reddan Group PLC department and program must conduct appropriate reviews and audits of their systems and processes to ensure compliance with internal policies and standards of Reddan Group PLC.

3.14 Breach of Policy

All Company Custodians are expected to report any real or suspected breaches of this Policy to the CISO, including any actual or suspected data breach involving personal or confidential information belonging to or within the possession, custody or control of Reddan Group PLC.

All incidents involving theft or loss of confidential information will be promptly addressed for containment, investigation, reporting, and remedial actions.