Data Management Policy

Policy Owner: Dan Pupek

Effective Date: 06/28/2022

Purpose

To ensure that information is classified, protected, retained, and securely disposed of in accordance with its importance to the organization.

Scope

This policy applies to all employees of Darwin Global or its divisions and its wholly-owned subsidiary and to all external parties with access to Darwin Global engineering data/information, information systems, networks, and system resources.

Policy

Darwin Global LLC classifies data and information systems in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Information systems and applications shall be classified according to the highest classification of data that they store or process.

Data Classification

To help Darwin Global LLC and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data.

Confidential

Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be passed to others with approval from the data owner, or a company executive. Example include:

- Customer Data
- Student Data
- Personally identifiable information (PII)
- Company financial and banking data
- Salary, compensation and payroll information
- Strategic plans
- Incident reports
- Risk assessment reports
- Technical vulnerability reports
- Authentication credentials
- Secrets and private keys
- Source code

- Litigation data

Restricted

Darwin Global LLC proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval. This is default for all company information unless stated otherwise. Examples include:

- Internal policies
- Legal documents
- Meeting minutes and internal presentations
- Contracts
- Internal reports
- Google Workspace Chat
- Email
- Student Data

Public

Documents intended for public consumption which can be freely distributed outside Darwin Global LLC. Examples include:

- Marketing materials
- Product descriptions
- Release notes
- External facing policies
- Blog posts
- Employee Biography's as approved by the employee

Labeling

Confidential data should be labeled "confidential" whenever paper copies are produced for distribution.

Data Handling

Confidential Data Handling

Confidential data is subject to the following protection and handling requirements:

- Access for non-preapproved-roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential Customer Data shall not be used or stored in non-production systems/environments
- Confidential data shall be encrypted in transit over public networks
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential data shall be protected by a log-on password or passcode and shall be configured to lock the screen after five (5) minutes of non-use
- Backups shall be encrypted
- Confidential data shall not be stored on personal phones or devices or removable media including USB drives, CD's, or DVD's
- Paper records shall be labeled "confidential" and securely stored and disposed
- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed

- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

Restricted Data Handling

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management and operations approval and shall only be done in accordance with a legal contract or arrangement, or the permission of the data owner
- Paper records shall be securely stored and disposed
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

Public Data Handling

No special protection or handling controls are required for public data. Public data may be freely distributed. Sites are encrypted via HTTPS.

Data Retention

Darwin Global LLC shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data. Retention periods shall be documented in the Data Retention Matrix in Appendix B to this policy.

Data & Device Disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. Darwin Global LLC shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third parties who meet Darwin Global LLC requirements for secure data disposal shall be used for storing and processing restricted or confidential data.

Darwin Global LLC shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of disposal.

Annual Data Review

Management shall review data retention requirements during the annual review of this policy. Data shall be disposed of in accordance with this policy.

Legal Requirements

Under certain circumstances, Darwin Global LLC may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by the Darwin Global LLC legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review with Darwin Global LLC's legal counsel to evaluate continuing requirements and scope.

Policy Compliance

Darwin Global LLC will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits.

Exceptions

Requests for an exception to this policy must be submitted to the Chief Software Architect, Information Systems Operations Manager, and the ISO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to any members or management or operations. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with the Darwin Global, LLC Employee Handbook, up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	06/29/2022	SOC2/2022	Diana Hussein	

APPENDIX A - Internal Retention and Disposal Procedure

Darwin Global LLC's Information Systems Operations Manager is responsible for setting and enforcing the data retention and disposal procedures for Darwin Global LLC's managed accounts and devices.

Customer Accounts:

1. Customer accounts and data shall be deleted within 60 days of contract termination through manual data deletion processes or in accordance.

Devices:

1. Employee devices will be collected promptly upon an employee's termination. Remote employees will be sent a shipping label and the return of their device shall be monitored.
2. Collected devices will be cleared to be re-provisioned—or removed from stock, Darwin Global LLC will securely erase the device.
3. Device images may be retained at the discretion of management for business purposes

Destroying devices or electronic media

In cases where a device is damaged in a way that Darwin Global LLC cannot access the Recovery Partition to erase the drive, Darwin Global LLC may optionally decide to use an E-Waste service that includes data destruction with a certificate. Darwin Global LLC will keep certificates of destruction on record for one year. Physical destruction can be optional if it is verified that the device is encrypted with Full Disk Encryption, which would negate the risk of data recovery.

Management will review this procedure at least annually.

APPENDIX B - Data Retention Matrix

System or Application	Data Description	Retention Period
Darwin Global LLC SaaS Products (Azure)	Customer Data	IAW contracted retention procedures or indefinite if not defined
Darwin Global LLC AutoSupport	Customer instance and metadata, debugging data	Indefinite
Darwin Global LLC Customer Support Tickets (Fogbugz)	Support Tickets and Cases	Indefinite
Darwin Global LLC Customer Support Phone Conversations (TalkDesk)	Support Phone Conversations	Indefinite
Darwin Global LLC Security Event Data (Azure)	Security and system event and log data, network data flow logs	On-Premise - Indefinite Azure Instance - 1 year
Darwin Global LLC Vulnerability Scan Data (Qualys)	Vulnerability scan results and detection data	6 months host (asset) data is retained until removed and purged from Qualys
Darwin Global LLC Customer Sales (Salesforce)	Opportunity and Sales Data	Indefinite
Darwin Global LLC QA and Testing Data (TestRail)	QA, testing scenarios and results data	Indefinite

Master Version: *https://docs.nexportsolutions.com/darwin-global-cyber-security-program/*