

Human Resources Security Policy

Policy Owner: Donna Reddout Effective Date: 06/29/2022

Purpose

To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.

Scope

This policy applies to all employees of Darwin Global LLC and its divisions, wholly owned subsidiary, consultants, contractors, and other third-party entities with access to Darwin Global production networks and system resources.

Policy Screening

Background screening on Darwin Global personnel shall be carried out in accordance with relevant laws and regulations and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Background screening shall include criminal history checks only after a conditional offer of employment., or as required by state or local statute. All third parties with technical privileged or administrative access to Darwin Global production systems or networks are subject to a background check or requirement to provide evidence of an acceptable background, based on their level of access and the perceived risk to Darwin Global.

Competence Assessment

The skills and competence of employees and contractors shall be assessed by human resources staff and the hiring manager or his or her designees as part of the hiring process. Required skills and competencies shall be listed in job descriptions and requisitions. Competency evaluations may include reference checks, education and certification verifications, technical testing, and interviews.

All Darwin Global employees will undergo an annual performance review which will include an assessment of job performance, competence in the role, adherence to company policies and code of conduct, and achievement of role-specific objectives.

Terms & Conditions of Employment

Company policies and information security roles and responsibilities shall be communicated to employees and third parties at the time of hire or engagement. Employees and third parties with access to company or customer information shall sign an appropriate non-disclosure or confidentiality agreement. Contractual agreements shall state responsibilities for information security as needed. Employees and relevant third parties shall follow all Darwin Global LLC information security policies.

Management Responsibilities

Management shall be responsible for ensuring that information security policies and procedures are reviewed annually, distributed, and available, and that employees and contractors abide by those policies and procedures for the duration of their employment or engagement. Annual

policy review shall include a review of any linked or referenced procedures, standards, or guidelines.

Management shall ensure that information security responsibilities are communicated to individuals, through written job descriptions, policies, or some other documented method that is accurately updated and maintained. Compliance with information security policies and procedures and fulfillment of information security responsibilities shall be evaluated as part of the performance review process wherever applicable.

Information Security Awareness, Education & Training

All Darwin Global employees and third parties with administrative or privileged technical access to Darwin Global production systems and networks shall complete security awareness training at the time of hire and annually thereafter. Management shall monitor training completion and shall take appropriate steps to ensure compliance with this policy. Employees and contractors shall be aware of relevant information security policies and procedures.

Disciplinary Process

Employees and third parties who violate Darwin Global's information security policies shall be subject to the Darwin Global disciplinary policies, up to and including termination of employment or contract.

Exceptions

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

Violations & Enforcement

Any known violations of this policy should be reported to any members of 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 company policies up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	06/30/2022	SOC2/2022	Diana Hussein	Donna Reddout