Email and Digital Resource Policy for Employee Recognition and Usage

1. Authority and Purpose

Pursuant to the authority vested in the Board of Trustees by the Trust Deed, this Policy establishes legally binding rules governing the provision, use, protection, and oversight of Official Email IDs and Official Digital Resources issued to employees of the Global Institute for Circular Economy and Sustainable Development Goals (NGO) (the "Institute") for the purpose of employee recognition and official communications.

2. Scope and Applicability

2.1 This Policy applies to all employees, consultants, interns, volunteers, contractors, and any other persons engaged by the Institute ("Relevant Persons").

2.2 All Official Email IDs and Official Digital Resources remain the sole property of the Institute and shall be used only in accordance with this Policy.

3. Definitions

3.1 "Official Email ID" means a unique electronic mail address issued by the Institute (e.g., name@krystahl.in OR name@krystahlesg.cloud or name@krystahl.com) for the exclusive purpose of official correspondence and recognition communications.

3.2 "Official Digital Resources" means digital assets, platforms, credentials, badges, business cards, certificates, computer system or any applications provided by the Institute to facilitate recognition of employee achievements and Institute-related communications.

3.3 "Data Breach" means any unauthorized access to, disclosure, alteration, destruction, or loss of data held in the Institute's Official Email or Official Digital Resources systems.

4. Issuance and Use

4.1 Assignment

(a) Upon commencement of engagement, each Relevant Person shall be assigned an Official Email ID and, where applicable, access credentials to Official Digital Resources.

(b) Access rights shall be proportionate to the individual's role and recognition-related responsibilities.

4.2 Permitted Use

(a) Official Email IDs and Official Digital Resources shall be used solely for Institute business and employee recognition functions, including peer nominations, award processing, official announcements, and related administrative tasks.

(b) Personal use of these resources is prohibited without express written authorization from the Human Resources Head.

4.3 Security Obligations

(a) Relevant Persons must maintain the confidentiality of login credentials and employ Institute-mandated security measures (e.g., strong passwords).

(b) Official communications and recognition data must be classified, transmitted, and stored in accordance with the Institute's Data Security Guidelines.

5. Data Security and Compliance

5.1 Regulatory Framework

The Institute and all Relevant Persons shall comply with:

(a) Information Technology Act, 2000;

(b) IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; and

(c) Other applicable Government of India data protection laws and regulations.

5.2 Data Breach Response

(a) Any actual or suspected Data Breach must be reported immediately—no later than twenty-four (24) hours—addressed to the Institute's Data Protection Officer on krystahl@krystahl.in

(b) The Data Protection Officer shall initiate an incident response, mitigation, and notification protocol in accordance with statutory timelines.

5.3 Consequences of Data Breach

(a) Relevant Persons found responsible for willful or negligent conduct leading to a Data Breach shall be subject to disciplinary action, up to and including termination of engagement.

(b) The Institute reserves the right to pursue civil remedies or criminal prosecution under Sections 43A and 72A of the Information Technology Act, 2000, which may include monetary penalties and/or imprisonment.

6. Monitoring and Audit

6.1 The Institute reserves the right to monitor, audit, and review all activity conducted via Official Email IDs and Official Digital Resources to ensure compliance with this Policy.

6.2 Monitoring shall be conducted in a manner consistent with applicable privacy laws and the Institute's internal audit procedures.

7. Disciplinary Measures

7.1 Violation of this Policy shall be grounds for corrective action, which may include:

(a) Suspension or revocation of access rights;

(b) Formal reprimand;

(c) Financial liability for losses incurred; and/or

(d) Termination of employment or engagement.

7.2 Disciplinary procedures shall comply with the Institute's Grievance and Disciplinary Policy and relevant employment laws

8. Amendments and Review

8.1 This Policy shall be reviewed at least biennially by the Policy Committee (comprising the Heads of Legal, Human Resources, IT, and Internal Audit).

8.2 Amendments require approval by the Policy Committee and ratification by the Board of Trustees before taking effect.

For details about the organisation, visit www.krystahl.in.

Policy approved by the Board of Trustees, GICE&SDGs (**Krÿstähl**).

Policy revised in April 2025.s

Approved by: *Shivaani V*
Name: Human Resource Manager
Date: 07 April 2025
Version: 3.0
Document ID: KRYS-04