Disciplinary Process Policy

Objective and Scope

The objective of this policy is to document how Prevision Research addresses the need for a disciplinary action process.

Where there is a need for disciplinary action, a formal process in line with legislation shall be followed with the aim of providing a fair and equitable outcome.

The scope of this policy includes allegations of an information security breach of legislation whether intended or unintended, misconduct or breach of any company policy will be considered as unsatisfactory performance and a disciplinary process may be initiated.

Roles, Responsibilities and Authorities

The Centre Manager or competent delegate is engaged in any process related to disciplinary action

A designated IT officer shall be nominated by the Operations Director to ensure the interests of information security are considered and enabled in all aspects of disciplinary action.

Where an exception or deviation from an expectation or plan occurs, the senior assigned role shall make the determination in terms of what is an acceptable change. The change management process may need to be enacted.

Legal and Regulatory

Title	Reference
The Telecommunications (Lawful Business practice)(Interception of Communications) Regulations 2000	www.hmso.gov.uk/si/si2000/20002699.htm
The Privacy and Electronic Communications (EC Directive) Regulations 2003	www.hmso.gov.uk/si/si2003/20032426.htm
Criminal Law Act 1967	https://www.legislation.gov.uk/ukpga/1967/58/introduction

ISO 27001/2 REFERENCES	ISO 27001: 2013 Clause ID	ISO 27002: 2013 Annex A ID	**ISO 27001: 2022 Clause ID**	**ISO 27002: 2022 Control ID**
Disciplinary process	7.0	7.2.3		6.4

Related Information

- Position Agreements or Position Descriptions
- Employment Contracts or Agreements
- Confidentiality Agreements – Included in induction documents

Disciplinary Process Policy

Policy

In relation to information security matters, employees are expected to conduct themselves in accordance with:

- IS documented policies and work practices,
- IS standards in respect to CIA.

They are expected to be responsible for the care of assets under their control, and abide by the laws of the UK in particular information security as it applies in all working jurisdictions.

Allegations of a breach of legislation whether intended or unintended, misconduct or breach of any company policy will be considered as unsatisfactory performance and a disciplinary process may be initiated.

Should a formal warning or termination of employment be a necessary outcome of a disciplinary process, an investigation shall occur and the outcome of the investigation will dictate what, if any, action is appropriate.

Disciplinary Process

The disciplinary process follows a 4 step process which may terminate at any stage on agreement by the parties involved:

Authorised: Executive Team representative and/or a company Director only.

Step 1: Notification

Verbal notification of a disciplinary action.

An investigation shall occur before proceeding further:

- Who/what/when/where did the incident happen?
- Was the incident intentional or unintentional?
- How significant was the breach?
- Was this a first offence?
- Has the person been trained?

Depending on the nature of the event including legal or regulatory repercussions, business impact, effect of harm on others, subsequent counselling may be offered and no further action taken.

Step 2: Warning (written notice 1)

A notice is issued followed by an offer of further remedial training or support measures according to circumstances of the event and requests by the involved parties.

Step 3: Warning (written notice 2)

Without resolution or agreed improvements, a further warning (written notice 2) issued with additional agreed actions and timelines for parties to act to prevent termination of employment are established and agreed.

Step 4: Termination (written termination letter 3)

Managing Director to be consulted and must approve the action.

Disciplinary Process Policy

Whilst in most cases a minimum of two warnings will apply, circumstances in a particular case may initiate summary dismissal. For example, the investigation may justify immediate termination for behaviour that constitutes serious misconduct and a breach of law.

Policy review

This policy shall be reviewed by the policy owner annually or immediately after a process change failure or a policy breach is known to have occurred. Refer below for the most recent review.

History table

Date	Rev No	Changes	Reviewed By	Approved By	Training Y/N