2

2C Plymovent's

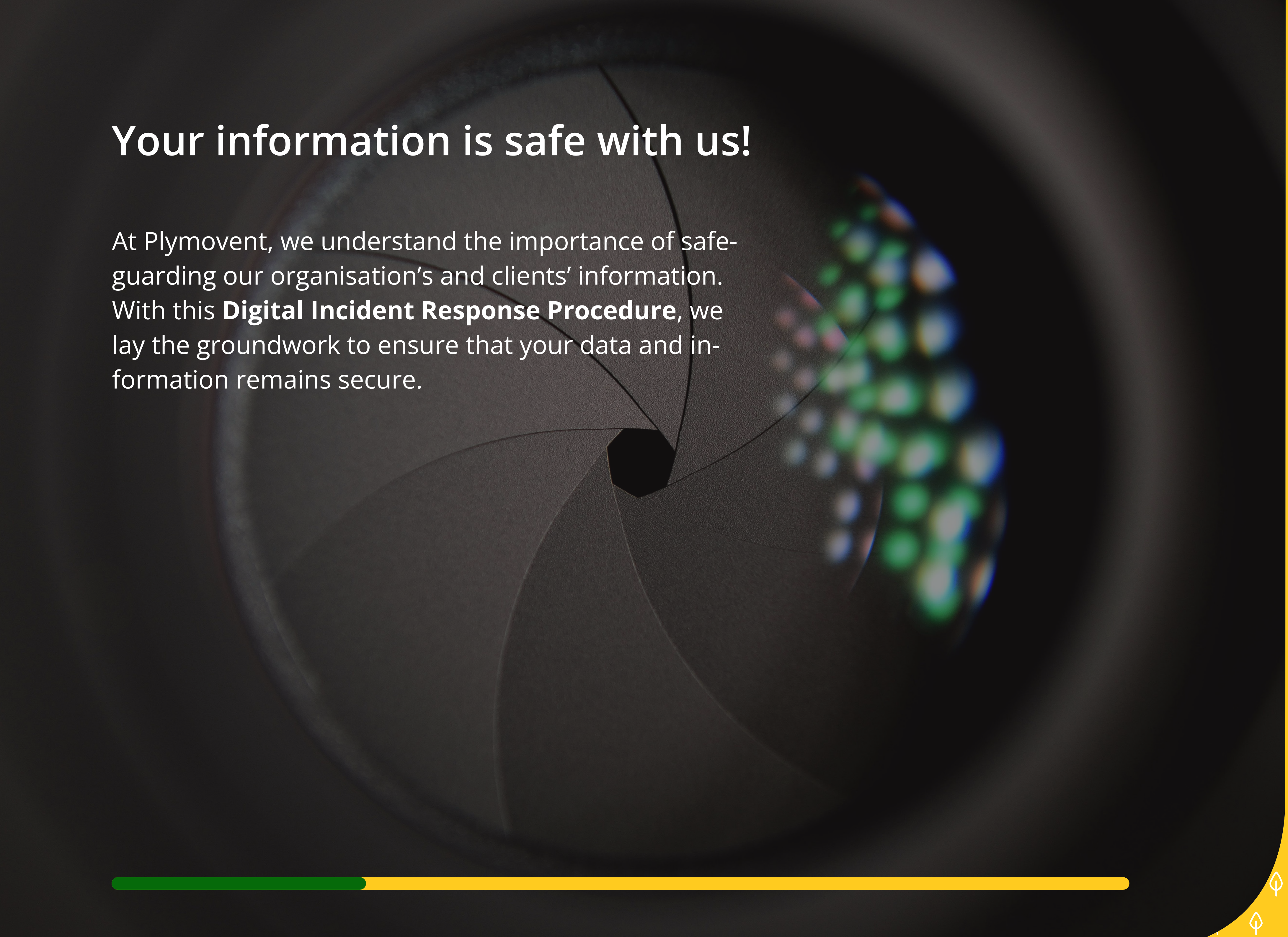
Digital Incident Response Procedure

Date of creation: January 2024
Date of review: March 2025
V202501

PLYMOVENT®
clean air at work

Your information is safe with us!

At Plymovent, we understand the importance of safeguarding our organisation’s and clients’ information. With this **Digital Incident Response Procedure**, we lay the groundwork to ensure that your data and information remains secure.



Maintaining a safe, secure, and resilient work environment

Shaping Plymovent's digital destiny

This **Digital Incident Response Procedure** provides employees with a step-by-step approach to handling and reporting data breaches or security incidents. It ensures swift resolution, minimal damage, and upholds the trust our clients place in us.

This procedure encompasses **everyone** who has a hand in shaping Plymovent's digital security, from our tech-savvy employees to our trusted contractors and third-party partners. It covers any situation that might jeopardize the **confidentiality, integrity, or availability** of our data. Every individual associated with Plymovent, **regardless of position**, has the right and responsibility to report any incidents, verbally or in writing.

Plymovent's
step-by-step approach to

Handle and report data breaches or security incidents

Handle and report data breaches or security incidents

1 First step: Report what you observed.

Begin with a **verbal report** to your immediate supervisor and Plymovent’s IT-manager.

Handle and report data breaches or security incidents

2 Next, we investigate.

Our investigation gears start turning and includes the following:

1. Initial report: Submit your verbal or written report to your superior or the Group IT-manager.

2. Initial assessment: We assess the severity of your incident. If possible, we'll try to resolve the matter without a formal investigation. If the superior or Group IT-manager does not proceed with a formal investigation, the reporting individual will be notified with the reasoning, in writing, within two weeks. We will also personally discuss potential threats or clarify any misunderstandings, if needed.

3. In case of formal investigation:

- The superior or Group IT-manager outlines the investigation procedure and possible actions. Information regarding any external support or resources.
- The superior and/or Group IT-manager conducts a thorough investigation, interviewing relevant individuals and reviewing associated materials or data.
- We'll update you on the progress once we are absolutely certain about the outcome. We'll certainly keep you informed of any progress or delays, as necessary.

Handle and report data breaches or security incidents

3 Let’s find a solution.

The **outcome** of the investigation will be communicated to all involved parties, either verbally or in writing.

- We’ll sit down to **share** what we found and the next steps to take.
- We’ll establish an **action plan** that outlines how we’re going to fix things, the timeline, and any remedial measures we need to put in place.

About this procedure

Let's stick to our procedure!
If someone chooses to disregard the policy, we may need to take appropriate action, e.g.:

- Formal warning
- Mandatory (corrective) training
- Termination of employment or contract
- Legal actions

Any questions? Please contact Group Management.

Policy Owner

Name Rene Bakker

Position Group Finance & IT

Date 01.03.2025

Location Alkmaar

Signature

PLYMOVENT®
clean air at work