



### Information on Cyber attacks

#### Context Description

Cyberattacks evolve every day. Their impact often remains hidden until they slow down operations or disrupt entire value chains.

At the same time, we connect our IT landscapes more tightly than ever. Electronic data interchange (EDI), virtual private networks (VPN), digital collaboration, and file exchange create new opportunities for cooperation.

They also open new paths for attackers who try to move from one company to the next. Modern malware already follows existing email conversations. It blends in so well that you hardly recognize the threat.

#### Objective

We at Innomotics believe that fast and clear incident communication keeps all of us protected when a cyberattack unfolds. It reduces unnecessary business impact and helps us react before an attack spreads.

This is why we ask you to contact our Cyber Defense Center as soon as you notice a cyber incident that could also affect us. We take every case serious and will handle it with full discretion.

#### Immediate Actions

Please share this information with everyone in your organization who protects your cybersecurity. This includes your CISO, CISO, CDC, SOC, CSIRT, CERT,... We also encourage you to send us the contact details of the teams or people who safeguard your IT infrastructure. Upfront. This allows us to reach out quickly if ever needed.

#### Additional Information

Innomotics GmbH cannot support you with specific technical actions to counter a security breach. You remain responsible for addressing your business risks and for acting quickly when a risk becomes reality.

### ⚠️ steps for Incident Handling

#### Inform Innomotics Cyber Defense Center

✉ [cert@innomotics.com](mailto:cert@innomotics.com)

☁ [innomotics.com/.well-known/security.txt](https://innomotics.com/.well-known/security.txt)

#### 1 provide the following information:

- Contact details
- Brief incident description
- Expected Impact

#### Optional:

- Response actions taken
- Upcoming remediation steps
- Indicators of compromise
- Request for remediation steps on our end
- TLP classification

#### 2 await response while mitigating

While you work on mitigating the cyberattack, our SOC evaluates the potential impact on Innomotics based on the information you share.

We might inform you if we plan to activate enhanced security measures on our side.

#### 3 update

We know your understanding of the situation will evolve during the investigation. We will agree with you on how to keep us updated, while giving us the time we need to remediate effectively.

### 🔍 Before an Incident

#### Share this document

Make sure everyone in your organization who plays a role in cybersecurity has access to this document and knows its content.

#### Print this document

Keep a printed copy of this document and the relevant contact details. This helps you stay prepared in case your IT systems become unavailable.