

EN

# Government Plan for Cyber and Digital Crisis Management

ENGLISH VERSION 12/09/2025

*Approved and made enforceable by the Government Council on September 12th, 2025.  
In case of discrepancy the French version shall prevail.*



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG

## Summary

|           |                                                    |           |
|-----------|----------------------------------------------------|-----------|
| <b>1.</b> | <b>Introduction</b>                                | <b>3</b>  |
| <b>2.</b> | <b>National and European framework</b>             | <b>4</b>  |
| <b>3.</b> | <b>Key concepts</b>                                | <b>5</b>  |
| 3.1.      | National classification of cybersecurity incidents | 5         |
| 3.2.      | Cyber threat classification                        | 5         |
| <b>4.</b> | <b>Cooperation modes</b>                           | <b>6</b>  |
| 4.1.      | Permanent mode                                     | 6         |
| 4.2.      | Alert/CERC mode                                    | 6         |
| 4.3.      | Crisis mode                                        | 6         |
| <b>5.</b> | <b>Crisis management bodies</b>                    | <b>7</b>  |
| 5.1.      | Cyber Risk Evaluation Cell (CERC)                  | 7         |
| 5.2.      | Crisis Cell (CC)                                   | 7         |
| 5.3.      | Cyber Operational Cell (PCO-C)                     | 8         |
| 5.4.      | Communication and Information Unit (CCI)           | 8         |
| <b>6.</b> | <b>Cyber or digital crisis management measures</b> | <b>10</b> |
| 6.1.      | Assessment                                         | 10        |
| 6.2.      | Enhanced monitoring                                | 10        |
| 6.3.      | System upgrade and protection                      | 10        |
| 6.4.      | Services restoration                               | 10        |
| <b>7.</b> | <b>International collaboration and assistance</b>  | <b>11</b> |
| <b>8.</b> | <b>Public information</b>                          | <b>11</b> |

# 1. Introduction

The Government Plan for Cyber and Digital Crisis Management establishes the overarching framework for the Luxembourg State's preparedness, coordination and response to cyber or digital events that could harm the vital interests or essential needs of all or part of the country or its population. This includes situations such as major technical failure or large-scale attacks against public and/or private sector information and communication technology systems.

This plan builds on the Cyber Emergency Response Plan (PIU Cyber) to ensure continued compliance and resilience against the evolving threat landscape and the national and European regulatory frameworks.

## **The main objectives of the plan are:**

- › to strengthen preparedness, prevention and protection against cyber and digital risks;
- › to define the governance principles and crisis management bodies necessary for effective national coordination;
- › to establish general procedures for responding to and managing crisis situations, as well as the respective roles of the actors involved;
- › to establish the framework for disseminating alerts from the authorities and information to the public.

It applies when an event is, or could become, serious enough to require urgent decisions and coordination at the national level and, where appropriate, coordination with European and international crisis management mechanisms.

A cyber or digital emergency refers to an event resulting from a cyber incident or threat that could cause major disruption to – or even the complete unavailability of – information and communication technology systems, affecting or likely to affect the vital interests or essential needs of all or part of the country or population of the Grand Duchy of Luxembourg.

This plan has been drafted and is managed by the High Commission for National Protection (*Haut-Commissariat à la protection nationale, HCPN*). Its operational execution is within the Government's remit. Depending on the nature and severity of the situation, relevant ministries, administrations and governmental departments are involved in cooperating to achieve defined goals, in accordance with the mandate of each stakeholder.

## 2. National and European framework

The plan is integrated into the national crisis management framework coordinated by the High Commission for National Protection (HCPN) and is aligned with European frameworks for cybersecurity and crisis management, in particular:

- › Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, known as the NIS 2 Directive;
- › The Council Recommendation of 6 June 2025 on an EU blueprint on cybersecurity crisis management ("Cyber Blueprint");
- › European crisis cooperation and coordination mechanisms such as the Integrated Political Crisis Response (IPCR) and the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe).

This positioning ensures consistency between Luxembourg's response and European approaches, in particular when cyber crises extend beyond national borders.

### 3. Key concepts

#### 3.1. National classification of cybersecurity incidents

To ensure a rapid, proportionate and coordinated response, the national framework distinguishes between:

- › **Large-scale cross-border cybersecurity incident:** an incident resulting in disruptions that exceed Luxembourg's response capabilities or which significantly impact at least one other Member State or third country;
- › **Large-scale national cybersecurity incident:** an incident resulting in disruptions detrimental to the vital interests or essential needs of all or part of the country or population, requiring urgent decisions and coordination;
- › **Significant incident:** an incident which
  - has caused, or is capable of causing, severe operational disruption to services or financial loss for the entity concerned;
  - has affected, or is capable of affecting, other natural or legal persons by causing considerable material or non-material damage.
- › **Incident:** an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems.

This classification is used to assess the scale of the incident and adapt the mode of cooperation and level of mobilization of the involved actors.

#### 3.2. Cyber threat classification

The plan distinguishes between several levels of cyber threats, based on their potential impact, scope and the nature of the targets, in order to anticipate the appropriate vigilance and cooperation measures.

## 4. Cooperation modes

The Government Plan for Cyber and Digital Crisis Management is founded upon three complementary cooperation modes.

### 4.1. Permanent mode

In the absence of crises, the plan operates in permanent mode. This mode is dedicated to preparation comprising:

- › Continuous monitoring of the cyber threat landscape and systemic risks;
- › Adapting and updating crisis plans and procedures;
- › Regular organisation of exercises and tests.

### 4.2. Alert/CERC mode

When an event presents a risk of significant harm without constituting an actual crisis, coordination is conducted in "Alert/CERC" mode. This mode ensures heightened vigilance, facilitates rapid and targeted information sharing among relevant stakeholders, and enables early implementation of mitigation measures to prevent any escalation into a crisis situation.

### 4.3. Crisis mode

When a cyber or digital event threatens vital interests or essential needs, "Crisis" mode is activated to ensure coordinated and efficient national management.

This mode enables the activation of planned response mechanisms, the structuring of information exchanges necessary for understanding and monitoring the event, and the coordination of cyber-response actions with other crisis management frameworks, whether sectoral, national or international.

## 5. Crisis management bodies

### 5.1. Cyber Risk Evaluation Cell (CERC)

The Cyber Risk Evaluation Cell (*Cellule d'Évaluation du Risque Cyber, CERC*) is responsible for analysing, assessing and monitoring cybersecurity incidents and cyber threats. It provides enhanced monitoring, assesses the severity and potential impact of events and, if required, formulates recommendations and defines next steps, such as escalating to "Crisis" mode.

### 5.2. Crisis Cell (CC)

In "Crisis" mode, crisis management relies on a governance structure adapted to the nature and scale of the event. The Crisis Cell (*Cellule de Crise, CC*) is activated by the Prime Minister in the event of an imminent or actual crisis. The Crisis Cell initiates, coordinates and monitors the execution of all measures intended to deal with the crisis and its effects, while facilitating a return to normalcy. It formulates the necessary crisis management decisions to be submitted to the Government for approval. In the event of operational intervention in the field, its mandate extends to coordinating and monitoring its implementation.

In an emergency situation, the Crisis Cell shall comprise at least the following stakeholders:

1. the High Commissioner for National Protection;
2. the Secretary General of the Government;
3. the Director General of the Grand-Ducal Police;
4. the Chief of Defence of the Luxembourg Armed Forces;
5. the Director of the State Intelligence Service (*Service de renseignement de l'État*);
6. the Director of the Government IT Centre (*Centre des technologies de l'information de l'État*);
7. the Director of the Department of Media, Connectivity and Digital Policy (*Service des médias, de la connectivité et de la politique numérique*);
8. the Director of the Luxembourg Regulatory Institute (*Institut luxembourgeois de régulation*);
9. a representative of the Ministry of the Economy;
10. a representative of the Ministry for Digitalisation.

The Crisis Cell operates throughout the duration of the crisis until normal conditions are restored.

Its membership may be expanded, depending on the circumstances and the topics to be discussed by representatives of other public entities, such as the Financial Sector Supervisory Commission (*Commission de Surveillance du Secteur Financier*), the Luxembourg Institute for Standardisation, Accreditation, Safety and Quality of Products and Services (*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*), the Directorate of Civil Aviation (*Direction de l'aviation civile*), ministries affected in the event of a cross-sector cyber crisis and affected municipalities, alongside representatives of operator/owners of critical infrastructure.

Should a member of the Crisis Cell be unable to attend, he must ensure to be represented by a designated alternate.

The Crisis Cell monitors situation developments based on information prepared on its behalf by the Cyber Operational Cell (PCO-C).

### **5.3. Cyber Operational Cell (PCO-C)**

The Crisis Cell may delegate the execution, implementation and monitoring of agreed measures and actions to the Cyber Operational Cell (*Cellule Opérationnelle Cyber, PCO-C*). The Cyber Operational Cell assumes the role of the Cyber Risk Evaluation Cell (CERC) and is additionally tasked with coordinating and implementing the agreed measures. It serves as the link between the strategic and technical levels.

### **5.4. Communication and Information Unit (CCI)**

The Communication and Information Cell (*Cellule Communication et Information, CCI*) is in charge of communication and information directed at the media and citizens. It is responsible for public and institutional communication and ensures that information provided to citizens, the media and stakeholders is clear, consistent and coordinated.

External communication is organised and horizontally coordinated by the Crisis Communication Department of HCPN (*Département Communication de crise*), focusing on preventing disinformation and ensuring consistency.

The Communication and Information Cell (CCI) convenes at the same time as the Crisis Cell. As regards the entities represented therein, the composition of the CCI reflects the composition of the CC, as closely as possible. The CCI regularly informs the public about the incident and its development, as well as the measures taken by the national authorities.

Official information is disseminated through the Government's institutional channels, in particular the [www.infocrise.lu](http://www.infocrise.lu) portal. Depending on the nature, severity and urgency of the situation, the Government may decide to use the national warning and information system LU-Alert, which enables rapid and targeted dissemination of essential information. Current alerts are communicated via the website [www.lu-alert.lu](http://www.lu-alert.lu), the **"LU-Alert" mobile application** and, where appropriate, via geolocated SMS and cell broadcast messages.

## **6. Cyber or digital crisis management measures**

The plan provides for crisis management measures that enable proportionate and flexible response to cyber or digital events, with the objective of protecting the vital interests of the country, its citizens and critical economic sectors.

### **6.1. Assessment**

Assessment is the first step in the crisis management cycle. It aims to assess the urgency of the event, its scale and its actual or potential impact on the vital interests or essential needs of all or part of the country or its population.

### **6.2. Enhanced monitoring**

Enhanced monitoring encompasses the actions taken when a situation presents an increased risk. These actions include analyzing available information and continuously assessing situational developments.

### **6.3. System upgrade and protection**

This measure aims to limit the risk of technical vulnerabilities being exploited and may result to the implementation of appropriate protection or mitigation measures, following the recommendation of the PCO-C and decision of the CC.

### **6.4. Service restoration**

Service restoration allows for the gradual resumption of affected activities, in line with defined priorities, until a normal and stable situation is restored.

## **7. International collaboration and assistance**

Given that a cyber crisis may have an international dimension, collaboration with foreign partners is crucial. International assistance may be requested, particularly through cooperation agreements with foreign incident response teams and within European and international organisations and cooperation networks.

## **8. Public information**

Providing information to the public is a core component of crisis management. The Government provides regular, coordinated updates regarding the evolution of the situation, its potential impacts and actions to be taken by citizens.

Official information is distributed via the Government's institutional channels, including the [www.infocrise.lu](http://www.infocrise.lu) portal. Depending on the nature, severity and urgency of the situation, the Government may use the national warning and information system LU-Alert, to ensure the rapid and targeted dissemination of critical information to the public.

In addition, any other communication channel deemed appropriate may be used to ensure that messages are distributed widely, quickly and reaching the broadest possible range of stakeholders.