TLP:AMBER

Limited distribution — share within your organisation on a need-to-know basis only. Do not share externally without authorisation. TLP: https://www.first.org/tlp/ | DK: https://www.cfcs.dk/da/handelser/traffic-light-protocol/

Defencial.dk

Crisis Communication Plan
CCP

Revision	*X.X*	**Classification**	**TLP:AMBER**
Responsible	*[Management Name]*	**Document Owner**	*[Owner]*

TEMPLATE GUIDANCE

This template is subject to modification so the plan fits the company's requirements and complies with applicable regulations. All grey italic text is draft example content — adapt it to your organisation before use. Remove all TEMPLATE GUIDANCE boxes before publishing.

Version History

Version	Date	Author	Change Description
1.0			Initial version

1 — Introduction

1.1 Purpose

TEMPLATE GUIDANCE

State why this plan exists. Link to business continuity policy, NIS2 Article 21/23, or GDPR Article 33/34 obligations where relevant.

[Company Name] is committed to transparent, timely, and accurate communication during any crisis affecting our operations, data, people, or reputation. This Crisis Communication Plan (CCP) establishes the structure, responsibilities, channels, and pre-approved messaging required to manage internal and external communication from the onset of a crisis to resolution.

The plan supports compliance with NIS2 reporting obligations (Article 23), GDPR breach notification requirements (Articles 33 and 34), and sector-specific regulatory requirements as applicable.

[Replace draft text above with your organisation's purpose statement]

1.2 Scope

TEMPLATE GUIDANCE

Define which types of crises are covered and which are out of scope. Examples: cyber incidents, data breaches, physical disasters, reputational events, supply chain failures, public health emergencies.

This plan applies to all crises that materially affect [Company Name]'s operations, personnel, customers, or public standing, including but not limited to:

- *Cyber incidents and data breaches (ransomware, unauthorised access, DDoS, insider threat)*
- *Personal data breaches requiring GDPR notification*
- *Significant service outages affecting customers or critical infrastructure*
- *Reputational events covered by media or social media*
- *Physical security incidents at company premises*
- *Supply chain failures affecting service delivery*

Out of scope: minor operational incidents that do not affect external stakeholders or regulatory thresholds.

[Adapt scope to your organisation. Define activation thresholds clearly.]

2 — Activation and Deactivation Criteria

TEMPLATE GUIDANCE *Define clear, objective criteria. Ambiguity here causes delay during real incidents. Get management agreement on these thresholds BEFORE an incident.*

2.1 Activation Criteria

This plan is activated when one or more of the following conditions are met:

[ ] A cyber incident has been confirmed that affects production systems, customer data, or business continuity
[ ] A personal data breach has occurred that may require GDPR Article 33/34 notification
[ ] An incident has been covered by, or is likely to be covered by, media or social media
[ ] A regulatory authority, law enforcement agency, or external stakeholder has made enquiries related to an incident
[ ] An incident has caused or is likely to cause physical harm or significant financial loss
[ ] The CISO, CEO, or Legal Counsel determines that coordinated communication is required
[ ] NIS2 early warning threshold is reached (significant incident per Article 23)

Activation authority:

The Crisis Communication Lead (SPOC) activates this plan upon notification from the CISO, CEO, Legal Counsel, or IR team. Outside business hours, the on-call manager has authority to activate.

[Adapt activation criteria to your organisation's context and risk tolerance]

2.2 Deactivation Criteria

This plan is deactivated when all of the following conditions are met:

[ ] The root cause has been identified and remediated
[ ] All affected parties have been notified as required
[ ] Regulatory reporting obligations have been fulfilled
[ ] Media and social media coverage has stabilised
[ ] No new significant developments are expected within the next 48 hours
[ ] Senior management and Legal Counsel have confirmed deactivation is appropriate

Upon deactivation: issue a final internal all-clear message. Initiate post-incident review within 5 business days. Retain all communication records as part of the incident file.

[Define who has authority to deactivate and what the formal close-out process is]

3 — Crisis Communication Team

SPOC RULE

The Crisis Communication Lead is the Single Point of Contact (SPOC) for all crisis communications. ALL external communication — to media, regulators, customers, or partners — must be approved by or channelled through this person. No one else speaks publicly about the incident without explicit authorisation.

3.1 Team Roster

Name	Role	Primary Phone	Email	Backup Contact
[SPOC Name]	Crisis Communication Lead			
[Name]	CEO / C-level Spokesperson			
[Name]	IT / CISO / DFIR Lead			
[Name]	Legal Counsel			
[Name]	HR Representative			
[Name]	PR / Communications Officer			
[Name]	DPO (GDPR)			

3.2 Responsibilities

TEMPLATE GUIDANCE

Define who does what. Overlap and ambiguity in roles during a crisis is costly. Pre-define and train on these responsibilities.

Role	Key Responsibilities
Crisis Communication Lead (SPOC)	Activates plan • Coordinates all messaging • Single external voice • Approves all statements • Manages media and regulator contact
CEO / C-level	Executive spokesperson for serious incidents • Final approval on public statements • Regulator and board liaison
CISO / DFIR Lead	Provides technical briefings to the team • Determines incident scope and severity • Advises on what can be disclosed
Legal Counsel	Reviews all external communications for legal risk • Advises on regulatory obligations • Manages law enforcement liaison
DPO	Leads GDPR breach assessment • Manages supervisory authority notification (Art. 33) • Advises on data subject notification (Art. 34)
HR Representative	Leads internal employee communication • Manages personnel-related aspects
PR / Communications	Drafts and distributes statements • Monitors media • Manages press enquiries

4 — Stakeholder Identification and Analysis

TEMPLATE GUIDANCE *Map all stakeholders and their communication needs BEFORE an incident. Update this matrix at least annually or when relationships change.*

Stakeholder Group	Representative / Contact	Channel	Key Message Priority
Employees			
Senior Management / Board			
Customers			
Media / Press			
Regulators / Authorities			
Suppliers / Partners			
General Public			

5 — Risk Assessment and Crisis Scenarios

TEMPLATE GUIDANCE *List the crises most relevant to your organisation. For each: what is the likely communication impact? Who needs to be notified and by when? NIS2 Article 23 requires early warning within 24 hours for significant incidents.*

Scenario	Likelihood (H/M/L)	Impact (H/M/L)	Communication Priority & Regulatory Trigger
Ransomware / destructive malware			Immediate SPOC activation. NIS2 early warning within 24h. GDPR assessment required.
Data breach (customer PII)			GDPR Art. 33 notification to DPA within 72h. Art. 34 if high risk to individuals.
DDoS / service outage			Customer notification if SLA breach. NIS2 if essential service disrupted.
Insider threat / employee misconduct			HR + Legal lead. Limited disclosure. Law enforcement if criminal.
Supply chain compromise			NIS2 supply chain risk. Partner notification. Customer impact assessment.
Physical security incident			Law enforcement. HR. Safety-first messaging.
Reputational / media event			PR lead. Rapid response within 1 hour of coverage appearing.

6 — Key Messages and Draft Statements

DRAFT TEXT

The statements below are draft examples in grey italic text. Adapt language, facts, and tone to your organisation before use. All statements must be reviewed and approved by Legal Counsel and the Crisis Communication Lead before release.

6.1 Core Message Principles

All crisis communications from [Company Name] will adhere to these principles:

1. *Accuracy: We only state what we know to be true. We do not speculate.*
2. *Transparency: We acknowledge the incident and what we are doing about it.*
3. *Empathy: We acknowledge the impact on affected parties.*
4. *Timeliness: We communicate early, even when information is incomplete, and update as we learn more.*
5. *Consistency: All spokespeople use approved language. No off-the-record comments.*

[Adapt core message principles to reflect your company's values and communication culture]

6.2 Initial Holding Statement (Generic — First 1–2 Hours)

TEMPLATE GUIDANCE

A holding statement buys time while facts are established. It must be ready to issue within 60 minutes of crisis activation. Replace [BRACKETS] with actual information before sending.

DRAFT HOLDING STATEMENT

[Company Name] is aware of [a cybersecurity incident / a service disruption / an issue] that came to our attention on [DATE] at approximately [TIME].

We have activated our incident response and crisis communication procedures. Our teams are working to understand the full scope of what has occurred and to restore normal operations as quickly as possible.

The security and integrity of our systems and the protection of our customers' data are our highest priorities.

We will provide an update by [TIME / DATE]. If you have immediate questions, please contact [CONTACT NAME / EMAIL / PHONE].

— [Company Name] Communications Team

6.3 Customer Notification — Data Breach

TEMPLATE GUIDANCE

Required under GDPR Article 34 when a breach is likely to result in high risk to individuals. Must be clear, plain language, and specific. Legal Counsel must review before sending.

DRAFT CUSTOMER NOTIFICATION

Subject: Important Security Notice from [Company Name]

Dear [Customer Name / Valued Customer],

We are writing to inform you of a security incident that may have affected your personal data.

What happened: On [DATE], [Company Name] discovered that [brief, factual description of what occurred — e.g. 'unauthorised access to our systems resulted in exposure of customer account data']. We immediately launched an investigation and engaged external cybersecurity specialists.

What data was affected: [Specific data types — e.g. name, email address, encrypted password. Do NOT speculate. Only include confirmed data types.]

What we have done: [Actions taken — e.g. contained the incident, notified authorities, engaged forensic investigators, applied security patches].

What you should do: We recommend you [e.g. change your password, be alert to phishing emails, monitor your account for unusual activity]. [Include specific steps relevant to the data type affected.]

We have notified [the relevant supervisory authority] as required by law.

If you have questions, please contact our dedicated response line: [EMAIL / PHONE / URL].

We sincerely apologise for any concern this may cause.

[Name], [Title]
[Company Name]

6.4 Internal Employee Statement

DRAFT INTERNAL STATEMENT

To: All Staff
From: [CEO / Crisis Communication Lead]
Subject: Important Update — [Incident Type]

We want to keep you informed about an incident that is currently being managed by our teams.

On [DATE], we became aware of [brief description]. We have activated our incident response procedures and are working to resolve this as quickly as possible.

What this means for you:
- *[Any actions staff should take — e.g. 'Do not access system X until further notice']*
- *[Any changes to working procedures]*
- *[Who to contact if you have questions or notice anything unusual]*

Important: Please do not discuss this incident externally or on social media. All enquiries from media, customers, or partners must be directed to [SPOC NAME / EMAIL].

We will update you by [TIME / DATE]. Thank you for your understanding and professionalism.

6.5 Media / Press Statement

DRAFT PRESS STATEMENT

[Company Name] Statement Regarding [Incident Type] — [DATE]

[Company Name] can confirm that [factual description of the incident, limited to confirmed facts only].

We identified the issue on [DATE] and immediately [actions taken — e.g. isolated affected systems, launched an investigation, notified relevant authorities].

We are working closely with [cybersecurity specialists / law enforcement / the relevant authority] to investigate the full scope of the incident and prevent recurrence.

[If data breach:] We take our obligations to our customers and data subjects seriously and are notifying affected individuals as required by applicable law.

We are committed to keeping our stakeholders informed and will provide further updates as the investigation progresses.

Media enquiries: [Press Contact Name], [Email], [Phone]

6.6 Regulatory Notification — NIS2 Early Warning (Within 24 Hours)

TEMPLATE GUIDANCE

NIS2 Article 23 requires an early warning to the national competent authority or CSIRT within 24 hours of becoming aware of a significant incident. This is NOT a full report — it is a brief initial notification. Full report follows within 72 hours.

DRAFT NIS2 EARLY WARNING

To: [National Competent Authority / CSIRT — e.g. CFCS / ENISA-registered authority]
From: [Company Name, Contact Name, Title, Email, Phone]
Date/Time (UTC): [DATE TIME]
Incident Reference: [Internal incident ID]

Early Warning Notification — NIS2 Article 23(1)

Organisation: [Company Name], [Sector], [Country]

Incident description (preliminary): [Brief factual description of what is known at time of notification. Do not speculate. State if investigation is ongoing.]

Estimated impact: [Scope, affected services, estimated number of users/customers affected if known]

Initial indicators: [Any known indicators of compromise, attack type if known (e.g. ransomware, supply chain), or state 'under investigation']

Cross-border impact: [Yes / No / Unknown — if Yes, specify affected member states if known]

Status: Investigation ongoing. Full incident notification to follow within 72 hours.

Contact: [Name, Title, Phone, Email]

7 — Communication Channels

TEMPLATE GUIDANCE *Document the actual channels your organisation uses. Note: if primary channels (email, intranet) are part of the affected system, you need out-of-band alternatives. Plan for this.*

Channel	Used For	Owner	Out-of-band Alternative
Company website / newsroom	Press releases, customer notices		*[Hosted externally? Independent CMS?]*
Corporate email	Customer notification, regulatory, staff		*[Phone tree / SMS if email compromised]*
Internal intranet	Employee updates		*[WhatsApp/Signal group, phone cascade]*
LinkedIn / social media	Public statements, brief updates		*[Pre-scheduled via Hootsuite etc.]*
Direct phone / SMS	Crisis team coordination		*[Always available — primary out-of-band]*
Press release wire (e.g. Cision)	Formal media distribution		*[Direct email to journalist list]*

OUT-OF-BAND If the incident affects your email or internal systems, you MUST have a pre-established out-of-band communication channel for the crisis team. Define this now. A Signal or WhatsApp group with all team members, or a pre-distributed phone cascade list, is the minimum.

8 — Media and Social Media Management

8.1 Media Guidelines

All media enquiries are directed to [PR Contact Name / Communications Lead]. No other employee is authorised to speak to media about a crisis without explicit approval from the Crisis Communication Lead.

When contacted by media before a statement is ready: 'Thank you for your enquiry. We are aware of the situation and are working to establish the full facts. We will issue a statement by [TIME]. Please contact [EMAIL] for updates.'

Do not confirm or deny details beyond the approved statement. Do not speculate. Do not discuss remediation details, technical vulnerabilities, or ongoing investigation status.

[Add your organisation's specific media guidelines and media contact list]

8.2 Social Media Strategy

Monitor: [Assign a named person] monitors [Twitter/X, LinkedIn, Facebook, local forums] for mentions of [Company Name] and the incident using [monitoring tool, e.g. Mention, Google Alerts, Brandwatch].

Response threshold: Respond to inaccurate information publicly within [2 hours]. Do not engage in argument. Refer to official statement URL.

Pause all scheduled posts immediately upon plan activation. Resume only after SPOC approval.

Social media tone: factual, calm, empathetic, consistent with approved statement. No humour. No speculation.

[Define monitoring responsibility, tools, and escalation criteria for social media]

9 — Internal Communication

9.1 Notification Cascade

Step 1: CISO / IR Lead notifies Crisis Communication Lead (SPOC) and CEO immediately upon crisis confirmation.

Step 2: SPOC activates crisis team via [phone / Signal / pre-defined channel] within 15 minutes.

Step 3: Legal Counsel and DPO notified simultaneously.

Step 4: All-staff notification issued within [60 minutes] of activation.

Step 5: Management briefing call convened within [90 minutes].

9.2 Update Schedule

During active crisis: internal updates every [2 hours / 4 hours] via [channel].

End of business day summary: mandatory unless crisis is resolved.

All-clear notification: issued by SPOC upon deactivation.

[Adapt notification cascade and update schedule to your organisation's structure]

10 — Training and Drills

Training frequency	*[Minimum: annually for full crisis team. New team members: upon joining.]*
Tabletop exercise	*[Scenario-based walkthrough of this plan. Include Legal, HR, CISO, Communications. Minimum annually.]*
Full simulation drill	*[Live exercise including mock media enquiry, regulator notification, and customer communication. Recommended every 2 years.]*
Post-drill review	*[Document lessons learned. Update plan within 30 days of exercise.]*
Training records	*[Who attended, date, outcome. Retain for audit/regulatory review.]*

11 — Monitoring and Evaluation

11.1 Monitoring Tools

Media monitoring	*[e.g. Google Alerts, Mention, Meltwater, Brandwatch — specify tool and responsible person]*
Social media monitoring	*[e.g. Hootsuite, Sprinklr, manual monitoring — specify cadence during active crisis]*
Regulator monitoring	*[Monitor for regulatory guidance, public statements, or queries related to the incident]*

11.2 Key Performance Indicators

Time to first public statement from crisis activation: target < 2 hours
NIS2 early warning issued within 24 hours: Yes / No
GDPR Article 33 notification issued within 72 hours: Yes / No
Media coverage tone: positive / neutral / negative (track over time)
Customer complaints received post-incident: count and category
Internal update adherence to schedule: % on time

[Adapt KPIs to your organisation's priorities and regulatory obligations]

12 — Review and Update

Review frequency	*Minimum: annually. After every activated incident. After significant organisational change.*
Owner of review	*[Name and role of plan owner]*
Revision procedure	*[How are changes proposed, reviewed, approved, and distributed? Who has edit access?]*
Distribution list	*[Who holds a copy of this plan? How are updates communicated?]*
Offline/printed copy	*[Is a hard copy maintained for use if systems are unavailable? Where is it stored?]*

13 — Approval and Sign-off

GOVERNANCE This plan must be reviewed and signed off by C-level management before it is considered active. It has no effect if it has not been approved and communicated to all team members.

Name	Role	Signature	Date

In a crisis, the plan you practised is the plan you execute. The plan you never opened is the plan that fails.