Ref. Ares(2026)10961481 - 24/11/2026

EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

ANNEXES 1 to 2

ANNEXES

to the

Commission Implementing Regulation (EU) .../...

laying down rules for the application of Directive (EU) 2022/2555 of the European Parliament and of the Council further specifying the type of information, the format and the procedure of a notification submitted pursuant to Article 23(1) of the Directive

ANNEX I

TEMPLATES FOR THE REPORTING OF SIGNIFICANT INCIDENTS

Part 1 - Significant incident early warning template

Field Code	Field Name	Short Description
A.1	Notification type	Type of incident notification or report being submitted to the competent authority.
A.2	Incident reference code provided by the competent authority	Unique reference code assigned by the competent authority at the time of receipt of the early warning report to unequivocally identify the significant incident.
A.3	Reporting date and time	Automatically-filled date and time at which the entity submitted the report of the significant incident.
A.4	Incident reference code assigned by the affected entity	Unique reference code issued by the entity to unequivocally identify the significant incident.
A.5	Name of the affected entity	Full legal name of the affected entity.
A.6	Entity type	Indication of whether the affected entity is essential or important, in accordance with Directive (EU) 2022/2555.
A.7	Primary contact person's name and surname	Name and surname of the primary contact person of the affected entity.
A.8	Primary contact person's email	Email address of the primary contact person.
A.9	Primary contact person's telephone	Telephone number of the primary contact person.
A.10	Second contact person's name and surname	Name and surname of the second contact person or the name of the responsible team within the entity.
A.11	Second contact person's email	Email address of the second contact person or the functional email address of the responsible team within the entity.
A.12	Second contact person's telephone	Telephone number of the second contact person, or of the responsible team within the entity.
A.13	Date and time at which the incident was detected	Date and time at which the entity became aware of the significant incident.
A.14	Date and time at which the incident occurred	Date and time at which the incident occurred.
A.15	Description of the incident	Description of the most relevant aspects of the significant incident.
A.16	Criteria that make the incident significant	Classification criteria that have triggered determination of the incident as significant and subsequent notification and reporting.
A.17	Sectors impacted	Indication of the sectors that have been affected by the significant incident.
A.18	Cross-border impact	Indication of whether the significant incident has affected other Member States.
A.19	Cross-border impact - countries	Member States impacted by the significant incident.
A.20	Incident caused by unlawful or malicious acts	Indication of whether the incident was caused by unlawful or malicious acts.
A.21	Support from national CSIRT required	Indication of whether support is required from the national CSIRT to respond to the incident.
A.22	Description of support required	Description of the support required to effectively respond to the incident.
A.23	Other national CSIRT or third country agency involvement	Indication of whether other national CSIRTs or agencies from other Member States or other countries have been notified or are actively providing assistance.
A.24	Other national CSIRT or third country agency involvement - countries	Indication of which other Member States or other countries have been notified or are actively providing assistance.
A.25	Significant incident reclassification	Reclassification from significant to non-significant incident if the significance threshold is not reached.
A.26	European Business Wallet details of the affected entity	Owner identification data, unique identifier and, where applicable, the digital addresses of the European Business Wallet of the entity, as issued in line with Regulation (EU) …/….

Part 2 - Significant incident notification template

Field Code	Field Name	Short Description
A.1	Notification type	Type of incident notification or report being submitted to the competent authority.
A.2	Incident reference code provided by the competent authority	Unique reference code assigned by the competent authority at the time of receipt of the early warning report to unequivocally identify the significant incident.
A.3	Reporting date and time	Automatically-filled date and time at which the entity submitted the report of the significant incident.
A.4	Incident reference code assigned by the affected entity	Unique reference code issued by the entity to unequivocally identify the significant incident.

A.5	Name of the entity affected	Full legal name of the affected entity.
A.6	Entity type	Indication of whether the affected entity is essential or important, in accordance with Directive (EU) 2022/2555.
A.7	Primary contact person's name and surname	Name and surname of the primary contact person of the affected entity.
A.8	Primary contact person's email	Email address of the primary contact person.
A.9	Primary contact person's telephone	Telephone number of the primary contact person.
A.10	Second contact person's name and surname	Name and surname of the second contact person or the name of the responsible team within the entity.
A.11	Second contact person's email	Email address of the second contact person or the functional email address of the responsible team within the entity.
A.12	Second contact person's telephone	Telephone number of the second contact person, or of the responsible team within the entity.
A.13	Date and time at which the incident was detected	Date and time at which the entity became aware of the significant incident.
A.14	Date and time at which the incident occurred	Date and time at which the incident occurred.
A.15	Description of the incident	Description of the most relevant aspects of the significant incident.
A.16	Criteria that make the incident significant	Classification criteria that have triggered determination of the incident as significant and subsequent notification and reporting.
A.17	Sectors impacted	Indication of the sectors that have been affected by the significant incident.
A.18	Cross-border impact	Indication of whether the significant incident has affected other Member States.
A.19	Cross-border impact - countries	Member States impacted by the significant incident.
A.20	Incident caused by unlawful or malicious acts	Indication of whether the incident was caused by unlawful or malicious acts.
A.21	Support from national CSIRT required	Indication of whether support is required from the national CSIRT to respond to the incident.
A.22	Description of support required	Description of the support required to effectively respond to the incident.
A.23	Other national CSIRT or third country agency involvement	Indication of whether other national CSIRTs or third country agencies have been notified or are actively providing assistance.
A.24	Other national CSIRT or third country agency involvement - countries	Indication of which other EU Member States or other countries have been notified or are actively providing assistance.
A.25	Significant incident reclassification	Reclassification from significant to non-significant incident if the significance threshold is not reached.
A.26	European Business Wallet details of the affected entity	Owner identification data, unique identifier and, where applicable, the digital addresses of the European Business Wallet of the entity, as issued in accordance with Regulation (EU) …./….
B.1	Observed and expected severity and impact of the incident	Description of the observed and expected impact and severity of the significant incident, including an assessment of the impact on: (a) the provision of services; (b) other entities within the sector and/or nationally; (c) upstream or downstream suppliers; (d) other entities within the same group.
B.2	Indicators of Compromise for this incident are available	Indication of whether the entity has access to information related to the significant incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.

Part 3 - Significant incident final report template

Field Code	**Field Name**	**Short Description**
A.1	Notification type	Type of incident notification or report being submitted to the competent authority.
A.2	Incident reference code provided by the competent authority	Unique reference code assigned by the competent authority at the time of receipt of the early warning report to unequivocally identify the significant incident.
A.3	Reporting date and time	Automatically-filled date and time at which the entity submitted the report of the significant incident.
A.4	Incident reference code assigned by the affected entity	Unique reference code issued by the entity to unequivocally identify the significant incident.
A.5	Name of the entity affected	Full legal name of the affected entity.
A.6	Entity type	Indication of whether the affected entity is essential or important, in accordance with Directive (EU) 2022/2555.
A.7	Primary contact person's name and surname	Name and surname of the primary contact person of the affected entity.
A.8	Primary contact person's email	Email address of the primary contact person.
A.9	Primary contact person's telephone	Telephone number of the primary contact person.
A.10	Second contact person's name and surname	Name and surname of the second contact person or the name of the responsible team within the entity.
A.11	Second contact person's email	Email address of the second contact person or the functional email

		address of the responsible team within the entity.
A.12	Second contact person's telephone	Telephone number of the second contact person, or of the responsible team within the entity.
A.13	Date and time at which the incident was detected	Date and time at which the entity became aware of the significant incident.
A.14	Date and time at which the incident occurred	Date and time at which the incident occurred.
A.15	Description of the incident	Description of the most relevant aspects of the significant incident.
A.16	Criteria that make the incident significant	Classification criteria that have triggered determination of the incident as significant and subsequent notification and reporting.
A.17	Sectors impacted	Indication of the sectors that have been affected by the significant incident.
A.18	Cross-border impact	Indication of whether the significant incident has affected other Member States.
A.19	Cross-border impact - countries	Member States impacted by the significant incident.
A.20	Incident caused by unlawful or malicious acts	Indication of whether the incident was caused by unlawful or malicious acts.
A.21	Support from national CSIRT required	Indication of whether support is required from the national CSIRT to respond to the incident.
A.22	Description of support required	Description of the support required to effectively respond to the incident.
A.23	Other national CSIRT or third country agency involvement	Indication of whether other national CSIRTs or third country agencies have been notified or are actively providing assistance.
A.24	Other national CSIRT or third country agency involvement - countries	Indication of which other Member States or third countries have been notified or are actively providing assistance.
A.25	Significant incident reclassification	Reclassification from significant to non-significant incident if the significance threshold is not reached.
A.26	European Business Wallet details of the affected entity	Owner identification data, unique identifier and, where applicable, the digital addresses of the European Business Wallet of the entity, as issued in accordance with Regulation (EU) …/….
B.1	Observed and expected severity and impact of the incident	Description of the observed and expected impact and severity of the significant incident, including an assessment of the impact on: (a) the provision of services; (b) other entities within the sector and/or nationally; (c) upstream or downstream suppliers; (d) other entities within the same group.
B.2	Indicators of Compromise for this incident are available	Indication of whether the entity has access to information related to the significant incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable.
C.1	Indication of the primary root cause category	High-level classification of the primary root cause of the significant incident.
C.2	Indication of the primary root cause sub-category	Detailed classification of the primary root cause of the significant incident.
C.3	Date and time at which the incident was resolved	Date and time at which the incident was resolved.
C.4	Mitigation measures taken or planned to be taken to recover from the incident and prevent re-occurrence of the incident	Indication of whether the entity has implemented (or plans to implement) measures to prevent the re-occurrence of the significant incident.
C.5	Exploited vulnerability, where applicable	Indication of the vulnerability identifier (for example, EUVD ID or CVE ID) of the exploited vulnerability. If no identifier is available, provide a brief description of the exploited vulnerability. Enter 'N/A' if the incident is not cyber-related.

ANNEX II

DATA GLOSSARY AND INSTRUCTIONS FOR THE REPORTING OF SIGNIFICANT INCIDENTS

Annex II lays down instructions to be followed by essential and important entities when completing the notification templates set out in Annex I

Data Field Code	Data Field	Description	Mandatory for Early Warning	Mandatory for Incident Notification	Mandatory for Final Report	Field Type
A.1	Notification type	Indication of the type of incident notification or report being submitted to the competent authority.	Yes	Yes	Yes	Choice: — early warning; — incident report; — final report.
A.2	Incident reference code provided by the competent authority	Unique reference code assigned by the competent authority at the time of receipt of the early warning report to unequivocally identify the significant incident.	No	Yes, where available	Yes	Alphanumeric
A.3	Reporting date and time	Automatically-filled date and time at which the entity submitted the report of the significant incident.	Yes	Yes	Yes	YYYY-MM-DDThh:mmZ
A.4	Incident reference code assigned by the affected entity	Unique reference code issued by the entity to unequivocally identify the significant incident.	No	No	No	Alphanumeric
A.5	Name of the entity affected	Full legal name of the affected entity.	Yes	No	No	Alphanumeric
A.6	Entity type	Indication of whether the affected entity is essential or important, in accordance with Directive (EU) 2022/2555.	Yes	No	No	Choice: — essential; — important.
A.7	Primary contact person's name and surname	Name and surname of the primary contact person within the entity.	Yes	No	No	Alphanumeric
A.8	Primary contact person's email	Email address of the primary contact person that can be used by the competent authority for follow-up communication.	Yes	No	No	Alphanumeric
A.9	Primary contact person's telephone	Telephone number of the primary contact person that can be used by the competent authority for follow-up communication. The telephone number shall be reported with all international prefixes (for example, +33XXXXXXXXX)	Yes	No	No	Alphanumeric
A.10	Second contact person's name and surname	Name and surname of the second contact person or the name of the responsible team within the entity	No	No	No	Alphanumeric
A.11	Second contact person's email	Email address of the second contact person or the functional email address of the responsible team within the entity that can be used by the competent authority for follow-up communication.	No	No	No	Alphanumeric

Data Field Code	Data Field	Description	Mandatory for Early Warning	Mandatory for Incident Notification	Mandatory for Final Report	Field Type
A.12	Second contact person's telephone	The telephone number of the second contact person, or of the responsible team within the entity, that can be used by the competent authority for follow-up communication. The telephone number shall be reported with all international prefixes (for example, +33XXXXXXXXX)	No	No	No	Alphanumeric
A.13	Date and time when the incident was detected	Date and time at which the entity became aware of the significant incident.	Yes	No	No	YYYY-MM-DDThh:mmZ
A.14	Date and time at which the incident occurred	Date and time at which the incident occurred.	No	No	Yes	YYYY-MM-DDThh:mmZ
A.15	Description of the incident	Description of the most relevant aspects of the significant incident. Entities shall provide a high-level overview of the following information such as possible causes, immediate impacts, systems affected, and others. Entities shall state, where known or reasonably expected, whether the incident impacts third-party providers or other entities, the type of provider or entity, and their name. In subsequent reports, the field content can evolve over time to reflect the ongoing understanding of the significant incident and to describe any other relevant information about the significant incident not captured by the data fields, including the internal severity assessment by the entity (for example, very low, low, medium, high, very high) and an indication of the level and name of the most senior decision structures involved in responding to the significant incident.	Yes	No	Yes	Alphanumeric
A.16	Criteria that make the incident significant	Classification criteria that have triggered determination of the incident as significant and subsequent notification and reporting.	No	No	Yes	Choice (multiple): — Number of users affected — Percentage of affected users — Duration of outage — Geographical spread — Direct financial loss — Non-material damage — Material damage — Reputational damage / Incident has received media coverage — Exfiltration of trade secrets or other sensitive

Data Field Code	Data Field	Description	Mandatory for Early Warning	Mandatory for Incident Notification	Mandatory for Final Report	Field Type
						information. — Incident is capable of causing the death of a natural person — Incident is capable of causing considerable damage to a natural person's health — Incident is capable of resulting in unauthorised access for suspected malicious purposes to network and information systems — None — Other (specify).
A.17	Sectors impacted	Indicate the sectors that have been affected by the significant incident. In case the full extent of the impact of the significant incident is not yet known, indicate the sectors that the affected entity belongs to.	Yes	No	No	Choice (multiple): — Energy; — Transport; — Banking; — Financial Market Infrastructure; — Health; — Drinking Water; — Waste Water; — Digital Infrastructure; — Public Administration; — Space; — ICT Service Management; — Postal and Courier Services; — Waste Management; — Manufacture, Production and Distribution of Chemicals; — Manufacture, Production and Distribution of Food; — Manufacturing; — Digital Providers; — Research; — Other (specify).
A.18	Cross-border impact	Indication of whether the significant incident has affected other Member States	Yes	No	No	Choice: — Yes, the incident affects at least two other EU Member States; — Yes, the incident affects only one other Member State; — No, the incident affects only the Member State receiving the report. — Uncertain.
A.19	Cross-border impact – Member States	Member States impacted by the significant incident	Yes, if visible	Yes, if visible	Yes, if visible	Conditionally visible, if 'Cross-border impact' is either of the 'Yes' responses. Choice (multiple) populated by Member State? and EFTA country names.
A.20	Incident caused by unlawful or malicious acts	Indication of whether the incident was caused by unlawful or malicious acts.	Yes	No	No	Choice: — Yes; — No; — Uncertain.
A.21	Support from national CSIRT required	Indication of whether support is required from the national CSIRT to respond to the incident.	No	No	No	Choice: — Yes; — No.

Data Field Code	Data Field	Description	Mandatory for Early Warning	Mandatory for Incident Notification	Mandatory for Final Report	Field Type
A.22	Description of support required	Description of the support required to effectively respond to the incident. Only displayed if 'Support from national CSIRT required' is 'Yes'.	No	No	No	Conditionally visible, if 'Support from national CSIRT required' is 'Yes' Alphanumeric
A.23	Other national CSIRT or third country agency involvement	Indicate whether other national CSIRTs or third country agencies have been notified or are actively providing assistance.	No	No	No	Choice: — No other national CSIRTs or third country agencies involved; — Yes - Other national CSIRTs or third country agencies notified; — Yes - Other national CSIRTs or third country agencies notified and actively providing assistance.
A.24	Other national CSIRT or third country agency involvement - countries	Member States or third countries that have received notification or are actively providing assistance.	Yes, if visible	Yes, if visible	Yes, if visible	Conditionally visible, if 'Other national CSIRT or third country agency involvement' is either of the 'Yes' responses. Choice (multiple) populated by a full list of country names
A.25	Significant incident reclassification	Reclassification from significant to non-significant incident if the significance threshold is not reached.	No	Yes, if applicable	No	Choice: — Yes; — Not applicable for this incident.
A.26	European Business Wallet details of the affected entity	Indication of whether the affected entity is the owner of a European Business Wallet and, if so, provision of owner identification data and unique identifier issued by the relevant authority, as well as the digital address, where applicable, that is assigned to the entity as part of the Business Wallets framework	No	No	No	Choice: - Yes; - Not applicable.
B.1	Observed and expected severity and impact of the incident	Description of the observed and expected impact and severity of the significant incident, including an assessment of the impact on: (a) the provision of services; (b) other entities within the sector and/or nationally; (c) upstream or downstream suppliers; (d) other entities within the same group.	No	Yes	Yes	Alphanumeric
B.2	Indicators of Compromise for this incident are available	Indication of whether the entity has access to information related to the significant incident that may help identify malicious activity within a network or information system (Indicators of Compromise, or IoC), where applicable. A positive indication could enable the CSIRT or, where applicable, the competent authority to contact the entity	No	Yes	No	Choice: — Yes; — No; — Not applicable for this incident.

Data Field Code	Data Field	Description	Mandatory for Early Warning	Mandatory for Incident Notification	Mandatory for Final Report	Field Type
		for this information via a secure channel. IoC information can include the following categories of data: (a) IP addresses; (b) URL addresses; (c) domains; (d) file hashes; (e) malware data (malware name, file names and their locations, specific registry keys associated with malware activity); (f) network activity data (ports, protocols, addresses, referrers, user agents, headers, specific logs or distinctive patterns in network traffic); (g) email message data (sender, recipient, subject, header, content);				
C.1	Indication of the primary root cause category	High-level classification of the primary root cause of the significant incident, including the following high-level categories: (a) cyber attacks; (b) system failures and software bugs ; (c) human error and operational mistakes; (d) third-party service provider, supply chain and utility issues; (e) physical and environmental issues.	No	No	Yes	Choice (single): — cyber attacks; — system failures and software bugs; — human error and operational mistakes; — third-party, service provider, supply chain and utility issues; — physical and environmental issues.
C.2	Indication of the primary root cause subcategory	Detailed classification of the primary root cause of the significant incident, including the following detailed categories linked to the high-level categories that are reported in data field C.1: 1. Cyber attacks (if selected, choose one of the following): (a) vulnerability exploitation; (b) malicious insider actions (excluding third parties, contractors); (c) ransomware or wiperware; (d) malware injection (other than ransomware or wiperware); (e) denial of service (DoS/DDoS); (f) compromised credentials or tokens, or credential stuffing (excluding third party-managed accounts); (g) social engineering, cyber fraud, or scam (for example, phishing, smishing, BEC); (h) exploitation of an agentic AI system; (i) other cyber attack (specify);	No	No	Yes	Choice (Single): — Cyber attacks: vulnerability exploitation; — Cyber attacks: malicious insider actions (excluding third parties, contractors); — Cyber attacks: ransomware or wiperware; — Cyber attacks: malware injection (other than ransomware or wiperware); — Cyber Attacks: denial of service (DoS/DDoS); — Cyber attacks: compromised credentials or tokens, or credential stuffing (excluding third party-managed accounts); — Cyber attacks: social engineering, cyber fraud, or scam; — Cyber attacks: exploitation of an agentic AI system; — Cyber attacks: other cyber attack (specify); — System failures and software bugs: software failure - update or patch failure; — System failures and

Data Field Code	Data Field	Description	Mandatory for Early Warning	Mandatory for Incident Notification	Mandatory for Final Report	Field Type
		2. System failures and software bugs (if selected, choose one or more of the following): (a) software failure - update or patch failure; (b) software failure - other software failure; (c) hardware failure; (d) resource exhaustion (for example, computer memory exhaustion, demand-driven bandwidth exhaustion); (e) other system failure or software bug (specify); 3. Human error and operational mistakes (if selected, choose one or more of the following): (a) faulty procedure, policy or work-instruction; (b) improperly executed deployment, operation, or change (excluding software update failures); (c) configuration error (system, network, software, or security control); (d) other human error or operational mistake (specify); 4. Third-party, service provider, supply chain and utility issues (if selected, choose one or more of the following): (a) malicious issues at third party (for example, cyber-attack, compromise of supplier-managed accounts, malicious third party actions); (b) non-malicious issues at third party (for example, system failures, supplier or utility issues, human error or operational mistakes); (c) software supply chain compromise; (d) utilities outage (for example, public power grid, telecom network outage, water supply); (e) other third-party, service provider, supplier or utilities issue (specify); **5.** Physical and environmental issues (if selected, choose one or more of the following): (a) natural disasters or phenomena (for example, floods, earthquakes, wildfires, severe weather, lightning, electromagnetic				software bugs: software failure - other software failure; — System failures and software bugs: hardware failure; — System failures and software bugs: resource exhaustion — System failures and software bugs: other system failure or software bug (specify); — Human error and operational mistakes: faulty procedure, policy or work-instruction; — Human error and operational mistakes: improperly executed deployment, operation or change (excluding software update failures); — Human error and operational mistakes: Configuration error (system, network, software or security control); — Human error and operational mistakes: other human error or operational mistake (specify); — Third-party, service provider, supply chain and utility issues: malicious issues at third party; — Third-party, service provider, supply chain and utility issues: non-malicious issues at third party; — Third-party, service provider, supply chain and utility issues: software supply chain compromise; — Third-party, service provider, supply chain and utility issues: utilities outage; — Third-party, service provider, supply chain and utility issues: other third-party, service provider, supplier or utilities issue (specify); — Physical and environmental issues: natural disasters or phenomena; — Physical and environmental issues: sabotage and deliberate physical damage (including arson, vandalism, theft of physical assets and deliberate cable cuts); — Physical and environmental issues: accidental physical damage; — Physical and environmental issues: other physical or environmental issues (specify).

Data Field Code	Data Field	Description	Mandatory for Early Warning	Mandatory for Incident Notification	Mandatory for Final Report	Field Type
		and solar storms); (b) sabotage and deliberate physical damage (including arson, vandalism, theft of physical assets and deliberate cable cuts); (c) accidental physical damage; (d) other physical or environmental issue (specify).				
C.3	Date and time at which the incident was resolved	Date and time at which the incident was resolved.	No	No	Yes	YYYY-MM-DD Thh:mm:ss
C.4	Description of any mitigation measures taken or planned to be taken to recover from the incident and prevent its re-occurrence	Indication of whether the entity has implemented (or plans to implement) measures to prevent the re-occurrence of the significant incident.	No	No	Yes	Alphanumeric
C.5	Exploited vulnerability, where applicable	Indication of the vulnerability identifier (for example, EUVD ID or CVE ID) of the exploited vulnerability. If no identifier is available, provide a brief description of the exploited vulnerability. Enter 'N/A' if the incident is not cyber-related.	No	No	No	Alphanumeric