/ EMERGENCY DOCUMENT — CONFIDENTIAL

INCIDENT RESPONSE BRIEFING PACK

What to do. Right now. In the first hour.

ISSUED BY	Acta Security // actasecurity.eu
JURISDICTION	EU — Portugal (ops)
IR CHANNEL	Chat on website / browser-based
RESPONSE	< 1 hour target / 24 · 7 · 365
DATA	EU-hosted · EU & ZA resident operators · EU chain of custody
VERSION	2026.06 / for client use

// CONTENTS

> *"Operators on the keyboard. Not consultants on the slide deck."*
>
> — ACTA SECURITY

// 01_FIRST_HOUR

First hour checklist.

Do these in order. Don't skip ahead. Don't reboot yet.

01 STAY CALM
Panic causes mistakes. You have time to do this correctly.

02 DON'T REBOOT
Rebooting destroys volatile evidence — RAM, active sessions, encryption keys in memory.

03 DON'T WIPE
Do not delete files, run 'rm', format drives, or reinstall the OS until Acta advises.

04 ISOLATE
Disconnect affected systems from the network. Pull the cable or disable Wi-Fi. Do NOT power off.

05 PRESERVE
Screenshot unusual processes, open connections, error messages. Photograph screens if needed.

06 STOP THE SPREAD
Identify adjacent systems. Block lateral movement: segment VLANs, revoke shared credentials.

07 CHANGE PASSWORDS
Rotate email, VPN, admin, and cloud console credentials — from a CLEAN, unaffected device.

08 LOG EVERYTHING
Write down what you saw, when, and who. Timestamps matter. Use a separate, unaffected device.

09 CONTACT ACTA
Open the chat on our website in your browser. Give: org name, what you see, when it started.

10 LEGAL / COMMS
Loop in legal counsel before any external statement. Don't post publicly or notify staff broadly yet.

04_DO NOT — THESE ACTIONS DESTROY EVIDENCE OR ALERT THE ATTACKER

- Reboot or power off affected systems before Acta advises.
- Notify all staff before confirmed facts — tips off the attacker, creates panic.
- Pay a ransom without legal and IR consultation.
- Use the compromised network or device to coordinate the response.
- Run AV scans or cleanup tools without instruction — they overwrite evidence.
- Delete logs, files, or any forensic artefacts — even 'temp' ones.
- Post on social media, Slack, or Teams about the incident.

// 02_GATHER

Information to gather.

Collect this before or while contacting Acta. Approximate is fine.

// INCIDENT BASICS

WHEN DID IT START?
Exact time if known, approximate if not — include time zone.

HOW WAS IT DISCOVERED?
Alert / user report / external tip / ransom note / anomaly.

WHAT SYSTEMS ARE AFFECTED?
Hostnames, IPs, cloud resources, SaaS accounts.

IS THE ATTACKER STILL ACTIVE?
Ongoing encryption / exfil / C2 beaconing — or historical?

HAS ANYTHING BEEN CHANGED?
Reboots, password resets, AV scans, deletions since discovery.

// ENVIRONMENT

CLOUD PROVIDERS
Azure / AWS / GCP — tenant IDs, subscription IDs, account numbers.

ON-PREM VS CLOUD SPLIT
Which systems are on-prem, which cloud, which hybrid.

IDENTITY PLATFORM
Active Directory, Entra ID, Okta, Google Workspace, etc.

SECURITY TOOLS DEPLOYED
EDR, SIEM, firewalls, DLP — what is running and what is logging.

BACKUP STATUS
Are backups intact and isolated from the affected network?

// INDICATORS OF COMPROMISE

UNUSUAL ACCOUNTS OR LOGINS
New admin accounts, logins from unknown IPs or unusual hours.

SUSPICIOUS PROCESSES / FILES
Names, paths, hashes if available.

NETWORK ANOMALIES
Outbound to unknown IPs, large unexpected data transfers.

RANSOM NOTE OR MESSAGE
Exact text and filename — do not delete. Screenshot it.

ATTACKER CONTACT DETAILS
Email, Telegram, onion URL — note exactly as found.

// REGULATORY CONTEXT

PERSONAL DATA INVOLVED?
Names, IDs, financials, health data of EU or other residents.

APPLICABLE REGULATIONS
GDPR, NIS2, DORA, PCI DSS, HIPAA — which apply to you?

SUPERVISORY AUTHORITY
Which DPA / competent authority are you registered with?

SECTOR CLASSIFICATION
Finance, health, energy, transport — regulators differ by sector.

⏱ REGULATORY CLOCK — START COUNTING FROM DISCOVERY

GDPR Art. 33: notify the supervisory authority within 72h. **NIS2:** 24h early warning + 72h full notification. **DORA:** 4h to report a major ICT-related incident once classified.

// 03_CONTACT

How to reach Acta.

One channel. Always open. No app, no account required.

PRIMARY CONTACT — BROWSER-BASED CHAT // NO APP REQUIRED

STEP 1 — **OPEN THE IR CHANNEL**
Open the chat on our website in any browser — works on desktop or mobile.

STEP 2 — **NO ACCOUNT NEEDED**
No phone number, no email, no registration. The channel is always open.

STEP 3 — **SEND YOUR FIRST MESSAGE**
State: organisation name // what you observe // when it started.

STEP 4 — **RESPONSE TIME**
An operator responds within 1 hour — typically faster. 24 / 7 / 365.

/ no phone number · no account · EU-hosted · data stays in Europe

// WHAT HAPPENS AFTER YOU CONTACT US

T+0 — **TRIAGE**
Operator assesses severity, scope, and active threat status from your description.

T+1H — **SCOPE CALL**
Structured intake: environment, indicators of compromise, blast radius.

T+4H — **IR PLAN**
Written plan: containment steps, evidence preservation, comms guidance.

T+24H — **CONTAINMENT**
Active containment: credential rotation, network segmentation, forensic imaging.

T+72H — **ERADICATION**
Root cause confirmed. Attacker access removed. Backdoors identified and closed.

T+7D+ — **RECOVERY**
Hardened rebuild. Detection rules. Post-incident report. Regulatory notification support.

IR CHANNEL
Chat on website

WEBSITE
actasecurity.eu

OPS BASE
Porto, Portugal · Remote EU & South Africa

A clean report is not the goal. A boring attack surface is. — Acta Security