DOCUMENTO PUBBLICO · 2026-09-21

# Piano di risposta agli incidenti

Classificazione, tempi di presa in carico, notifiche alle autorità

**SEMPI S.r.l. — Società Benefit**

Terrazza Solferino, Via Davide Bertolotti n. 7, 10121 Torino (TO), Italia

P. IVA IT12315280011 · REA TO-1280911 · PEC sempi@legalmail.it

© 2020–2026 SEMPI S.r.l. — Società Benefit. Tutti i diritti riservati.

# Incident Response Plan — DORA + NIS2 Compliance

**Version:** 1.0.0

**Effective:** 2026-07-14

**Owner:** Compliance Officer (Claude / Liana)

**Review Frequency:** Quarterly (Sep 14, Dec 14, Mar 14)

---

## I. INCIDENT CLASSIFICATION & SLA

### Severity Levels

| Severity | Criteria | Response Time | Escalation | Regulatory Notice |
|---|---|---|---|---|
| **CRITICAL (S1)** | Data breach >100 users OR uptime loss >2h (99.99% SLA violated) OR unauthorized access to fiscal data | **1 hour** to Slack #incidents + PagerDuty | Owner + Compliance Officer + External Security | **24h** to competent authority (Agcom if NIS2 operator) |
| **HIGH (S2)** | Service degradation 30min-2h OR single-user data access incident OR failed audit trail (log loss/corruption) | **4 hours** to Slack | Team Lead + Compliance | None (internal log only) |
| **MEDIUM (S3)** | Minor data inconsistency (auto-resolved <1h) OR failed backup (redundancy OK) OR minor security alert | **Next business day** to Slack | Team | None |

### Examples

`

CRITICAL:

→ Hacker gains access to production DB (data breach)

→ API down for 2+ hours (99.99% SLA = max 21.6 sec/month)

→ Invoice PDF encryption key leaked

→ Audit log table corrupted

HIGH:

→ Invoice upload slow (>30sec) for 1 hour, auto-resolved

→ Customer reports they can see another company's VAT register

→ Backup job fails but 2 other backups succeeded

→ Brute force attack blocked by rate limiting

MEDIUM:

→ Duplicate invoice entry (caught in review, corrected)

→ Sentry error spike (not affecting users)

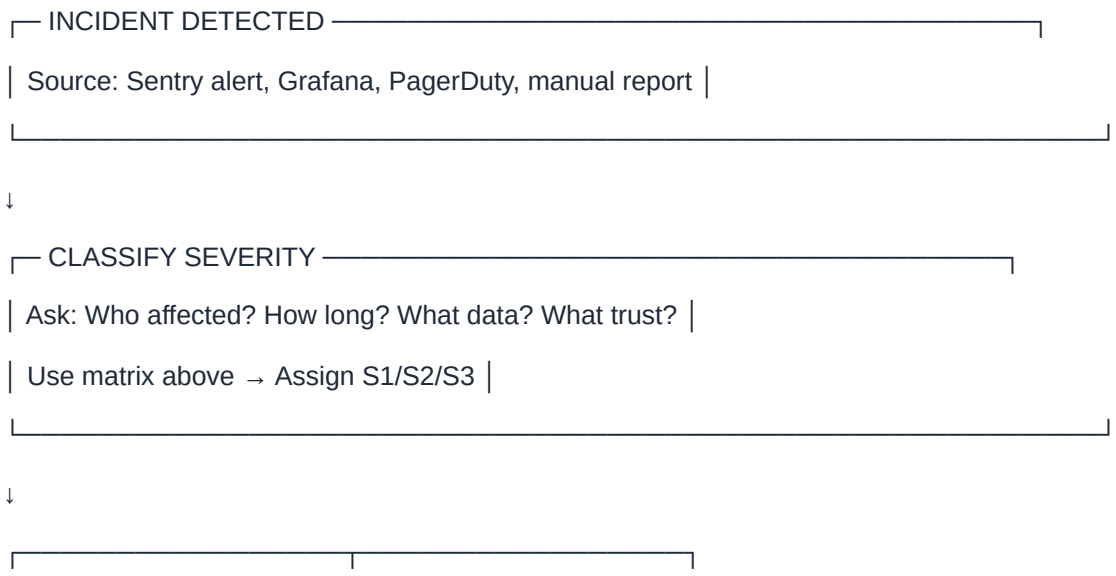
→ Certificate expiry warning (not yet expired)

`

---

## II. DETECTION & CLASSIFICATION FLOW

`



(24h)

`

---

## III. RESPONSE PLAYBOOK BY SEVERITY

### S1 (CRITICAL) — 1-Hour Response

**First 5 minutes:**

1. Trigger alert: Post message in Slack #incidents with `@channel`

`

🚨 CRITICAL INCIDENT #ID-001 — Data Breach Detected

Severity: CRITICAL (S1)

Time detected: 2026-07-14T09:15:32Z

Estimated impact: >100 users / fiscal data exposure

Owner: [On-call engineer]

Status: INVESTIGATING

`

2. Trigger PagerDuty → escalate to on-call engineer + manager

3. Start incident war room:

- Slack thread in #incidents

- Google Meet (link pinned to thread)

**First 30 minutes:** 4. Triage & containment:

- Identify affected systems / users / data
- Is the breach still ongoing? STOP it immediately
- Take snapshots (logs, affected data, access patterns)
- **Do NOT delete evidence** → preserve for forensics

5. Notify internal stakeholders:

- CEO / Compliance Officer

- Technical Lead

- Customer Support (prepare customer notification)

**30 min - 1 hour:** 6. Prepare regulatory notification:

- Summarize: what happened, who affected, when, impact
- Document remediation action taken
- Prepare for 24h submission to Agcom (if NIS2 operator)

**By 1 hour:** 7. Post update in #incidents:

```
🚨 UPDATE — Breach Contained

Status: CONTAINED

Affected users: [N]

Root cause: [brief]

Next: customer notification + forensics

ETA for full remediation: [date/time]
```

**24-72 hours:** 8. Regulatory submission (if required):

- File incident report with Agcom
- Include containment measures
- Include timeline + impact

**Post-incident (within 1 week):** 9. Root cause analysis (RCA):

- How did it happen?
- Why did detection fail?
- What layers of defense failed?
- Corrective actions?

10. Forensic audit:

- Review audit logs (did we catch all access?)

- Review backup (do we have clean copy?)

- Test incident recovery process

**S2 (HIGH) — 4-Hour Response**

**First 15 minutes:**

1. Post in Slack #incidents (no `@channel`, just #incidents subscribers)

2. Notify team lead

3. Document in incident_log table

**First 4 hours:** 4. Investigate root cause 5. Implement fix or workaround 6. Test fix 7. Deploy fix 8. Verify incident resolved

**Post-incident:** 9. Document in incident_log with fix details

**S3 (MEDIUM) — Next Business Day**

1. Log to incident_log table (automated)

2. Review in next standup

3. Fix on normal sprint schedule

---

## IV. AUTOMATED ALERTING

### Sentry → Slack Integration

```typescript
// server/sentry.ts
Sentry.init({
dsn: process.env.SENTRY_DSN,
environment: process.env.NODE_ENV,
beforeSend(event, hint) {
// Classify by severity
const severity = classifySeverity(event, hint);
if (severity === 'CRITICAL') {
// Post to Slack with @channel
postSlackAlert(event, severity, true);
triggerPagerDuty(event);
} else if (severity === 'HIGH') {
// Post to Slack without @channel
postSlackAlert(event, severity, false);
}
return event;
},
});
```

### Key Alerts to Monitor

```
CRITICAL:
- Uncaught exception in auth middleware (security bypass?)
- Multiple failed login attempts from same IP (brute force)
- Database connection timeout (service down)
```

- Tenant schema access denied (isolation violation)

- Audit trail table error (data integrity)

HIGH:

- Invoice API latency >5s (15+ errors)

- Failed vault access (encryption key unavailable)

- Memory usage >90% (potential crash)

- Rate limit threshold crossed

MEDIUM:

- Warnings (non-blocking errors)

- Performance degradation (slow but working)

- Test coverage below threshold

```

---

## V. INCIDENT LOG TABLE

```sql

CREATE TABLE IF NOT EXISTS incident_log (

id SERIAL PRIMARY KEY,

incident_id VARCHAR(20) UNIQUE NOT NULL, -- INC-001, INC-002, etc.

severity VARCHAR(20) NOT NULL, -- CRITICAL, HIGH, MEDIUM

title VARCHAR(255) NOT NULL,

description TEXT,

systems_affected TEXT[], -- ['api', 'db', 'auth']

users_affected INTEGER, -- Number of impacted users

-- Timeline

detected_at TIMESTAMP NOT NULL,

reported_at TIMESTAMP NOT NULL,

acknowledged_at TIMESTAMP,

contained_at TIMESTAMP,

resolved_at TIMESTAMP,

-- Response

response_time_minutes INTEGER, -- How long until response?

mttr_minutes INTEGER, -- Mean Time To Recovery

on_call_engineer VARCHAR(255),

-- Impact

estimated_data_loss TEXT,

users_notified BOOLEAN DEFAULT FALSE,

regulator_notified BOOLEAN DEFAULT FALSE,

regulator_notification_id VARCHAR(100), -- Agcom ref #

-- Forensics

root_cause TEXT,

corrective_actions TEXT,

audit_log_search_query TEXT, -- Query to find affected records

-- Metadata

post_mortem_link VARCHAR(500), -- Google Doc RCA

lessons_learned JSONB,

created_at TIMESTAMP DEFAULT NOW()

);

`

---

## VI. NOTIFICATION TEMPLATES

**Slack Alert (CRITICAL)**

`

🚨 **CRITICAL INCIDENT** 🚨

Severity: CRITICAL (S1)

Incident ID: INC-001

**What:** [One-line description]

**Who:** ~100 users affected

**When:** 2026-07-14 09:15 UTC

**Impact:** [Fiscal data exposed / service down / breach]

**Immediate action taken:**

- [Containment step 1]
- [Containment step 2]

**Next steps:**

- Forensics investigation
- User notification
- Regulatory filing (if required)

**War room:** [Google Meet link]

**On-call:** @engineer_name

**Compliance:** @compliance_officer

Updates in thread 👇

`

**Customer Notification Email (CRITICAL)**

`

Subject: Important Security Notice — Action Required

Dear [Customer],

We are writing to inform you of a security incident that affected your account on [date/time].

**What happened:**

[Explain in non-technical terms]

**What data was affected:**

[List specific documents/data]

**What we did:**

- Immediately contained the breach
- Reviewed access logs
- No unauthorized changes were made to your documents

**What you should do:**

1. [Action 1: e.g., reset password]

2. [Action 2: e.g., review recent activity]

**Support:**

If you have questions, contact us at security@sempifinance.it

We apologize for the incident. We are committed to your security.

Regards,

Sempifinance Security Team

`

---

## VII. QUARTERLY INCIDENT DRILLS

**Schedule:** First Monday of each quarter (Sep 4, Dec 2, Mar 3)

**Drill Scenario:** Simulated incident (e.g., "API down for 30 min")

**Participants:** Engineering, Operations, Compliance, Support

**Goals:**

1. Test Slack alerting pipeline

2. Verify PagerDuty escalation

3. Practice incident classification

4. Validate RCA process

5. Time response (is it < SLA?)

**Output:** Drill report in `/docs/compliance/incident-drills/`

---

## VIII. COMPLIANCE CHECKLIST

- [ ] Sentry alerts configured for CRITICAL + HIGH events
- [ ] PagerDuty integration tested (sends alerts to on-call)
- [ ] Slack #incidents channel created + alerts subscribed
- [ ] incident_log table created in DB
- [ ] War room setup (Google Meet auto-link in Slack alerts)
- [ ] Notification templates stored (Slack, email, regulatory)
- [ ] Incident drill scheduled (quarterly)
- [ ] Regulator contact list maintained (Agcom email/phone)
- [ ] Post-mortem RCA process documented
- [ ] All team members trained on incident response (annual)

---

## IX. CONTACT LIST

| Role | Name | Email | Phone | On-Call |
|---|---|---|---|---|
| ---------- | ---------- | -------------------------- | ---------- | --------- |
| Owner | Liana | liana@sempifinance.it | +39 02 XXXX | Primary |
| CTO | [Name] | cto@sempifinance.it | +39 02 YYYY | Secondary |
| Compliance | Claude | compliance@sempifinance.it | N/A | Tertiary |
| Agcom Contact | [Regulator] | [regulatory email] | [phone] | N/A |

---

**Next update:** 2026-10-14 (quarterly review)

**Last tested:** [Date of last drill]

**Status:** ACTIVE

> **Sorgente:** docs/compliance/INCIDENT_RESPONSE_PLAN.md
> **SHA-256 del sorgente:** 7975f99c85881be3490f2d799a41564560acf384a364cc463d51d6a8eb246ec9
> La data certa di questo documento è data dalla marca temporale qualificata incorporata nel PDF (PAdES, Reg. UE 910/2014). L'impronta qui sopra identifica il testo di partenza nel repository.