**Incident Response Plan Outline**

**1. Introduction**
The introduction should describe the purpose of the plan, its scope, its audience, and any defined terms used in the plan.

**2. Incident Severity Levels**
This is where incident severity levels are defined, and whether any external frameworks are used, like the ENISA recommendations on incident severity: https://www.enisa.europa.eu/publications/dbn-severity.

**3. Roles and Responsibilities**
This section identifies the members of the incident response team. It also assigns responsibilities to each of those members to ensure all aspects of the incident are handled. Be sure to think about how roles and responsibilities work when more than one region or operating division is involved, as applicable.

**4. Communications and Notifications (Internal and External)**
Communications should focus on both internal:

- Incident response team - including working with Legal to maintain attorney-client privilege
- C-suite
- Employees
- Affiliate companies

And external:

- Clients
- Vendors
- Media
- Regulators
- Law enforcement

This section should also take into account whether communications are required by law and/or contract.

**5. Security Incident Response Life-Cycle Phases**

- Incident intake and triage – how should initial reports be received and investigated?
- Incident validation – how to decide whether a report rises to the level of an incident?
- Plan Activation – how is the plan activated?
- Stakeholder Notifications – how is the incident response team made aware of the incident?
- Incident Response – how is the incident analyzed and contained?
- Incident Management – the ongoing day-to-day of how the incident is managed. Individual responsibilities should be detailed in section 3 above.
- Plan deactivation and post-mortem

**6. Appendices**

Include any additional supporting documents or references (e.g., incident tracking template, lists of key vendors, expense tracking template, team contact lists, related policies, etc.)