1. SCOPE OF WORK

The scope and objectives of the IR plan identify critical assets, potential threats, and the stakeholders involved:

- **Develop a cyber security incident response plan outlining the steps taken during and after an attack, helping minimize damage, restore operations swiftly, and ensure compliance with legal and regulatory requirements.**
- **Define overlap between IT incident ITIL and cyber incident process.**
- **Establish an incident response team with clearly assigned roles and responsibilities, ensuring all members are trained and equipped to act swiftly during an incident.**
- **Detailed procedures for incident detection, analysis, containment, eradication, and recovery.**
- **Set up communication protocols, escalation paths, and documentation requirements for every phase of the response process.**
- **Ensure compliance with relevant legal and regulatory obligations, such as data breach notification requirements and evidence preservation for potential investigations.**
- **Conduct tabletop exercises and simulated attacks, to validate and refine the IR plan.**
- **Communication plan, notification templates, stakeholder contact list, regulatory reporting templates, and communication logs.**

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1.1. Deliverables

No.	Functional Requirement	Description	Deliverables
1.	Incident Detection and Reporting	Process to detect, log, and report security incidents promptly. Clearly define criteria for incidents and set escalation procedures for staff.	Incident reporting process and procedure, incident register, escalation matrix, alerting use cases, and sample incident tickets.
2.	Incident Assessment and Classification	Implement structured procedures for evaluating and classifying incidents according to their severity, impact, and regulatory significance.	Incident classification standard, severity matrix, triage checklist, and completed classification records.
3.	Incident Response Team and Roles	Formalize the assignment, documentation, and training of incident	Incident response team charter, RACI matrix, role descriptions, contact list.

		response roles and responsibilities, ensuring comprehensive stakeholder inclusion.	
4.	Response Procedures	Develop detailed, stepwise procedures for addressing common incident types, including containment, eradication, recovery, and communication protocols.	Scenario-based playbooks, containment procedures, recovery procedures, and decision logs.
5.	Notification and Communication plan	Establish a formal communication framework for internal and external stakeholders, including regulatory notification requirements to authorities and affected individuals.	Communication plan, notification templates, regulatory reporting templates, and communication logs.
6.	Evidence Preservation and Forensics	Define procedures for the collection, preservation, and forensic analysis of digital evidence to support investigations and legal compliance.	Forensic procedure, evidence register, chain-of-custody forms, evidence inventory, and forensic analysis reports.

7.	Integrate with Legal and Regulatory Requirements	Ensure all incident response activities are aligned with applicable legislation and contractual obligations, with legal counsel engagement as appropriate.	Legal and regulatory obligations register, breach assessment template, notification decision log, legal review records, and retained compliance evidence.
8.	Post-Incident Review and Improvement	Conduct structured reviews following incidents to identify lessons learned and update response strategies, controls, and training program accordingly.	Post-incident review template, lessons learned report, root cause analysis, corrective action register, and updated procedures.
9.	Awareness and Training	Personnel understand their responsibilities in incident response processes.	Training plan, IR, awareness materials, competency assessments, and role-based training records.

10.	Continuous Improvement	Schedule regular, simulated attacks—and ensure continuous updates to maintain regulatory compliance and operational readiness.	Three scheduled, tabletop exercise packs, simulation reports, issue log, remediation tracker, and updated IR plan.

1.2. Acceptance criteria

All documents, models, processes, templates, and related deliverables must be provided in editable, reusable, and, where applicable, both Microsoft and open formats. Acceptable formats include DOCX or ODT for text documents, XLSX, XLSM, or ODS for spreadsheets and working models, PPTX or ODP for presentations, VSDX or SVG for diagrams and vector graphics, CSV for tabular data, XML and JSON for structured data exchange, and PDF only as a reference copy and not as the sole deliverable format.

The Supplier grants Sentech a perpetual, irrevocable, non-exclusive, royalty-free right to use, reproduce, adapt, modify, maintain, and internally distribute all deliverables for its own business, operational, governance, audit, compliance, and continuity purposes.