INCIDENT CHECKLIST.

HAS THE INCIDENT BEEN ASSESSED?

- Has the nature and scope of the incident been determined? .... □
- Have the impacted systems and data been identified? .... □
- Has the potential impact of the incident been estimated? .... □

HAVE THE APPROPRIATE STAKEHOLDERS BEEN NOTIFIED?

- Has the incident response team (IRT) been activated? .... □
- Has senior management been notified? .... □
- Have legal and regulatory authorities been notified? .... □

HAS THE INCIDENT BEEN CONTAINED?

- Have the affected systems been isolated? □
- Have affected accounts been disabled? □
- Has malicious traffic been blocked? □

HAS THE INCIDENT BEEN ELIMINATED?

- Has the malware or other threat been removed from the system? □
- Have any vulnerabilities been patched? □
- Has the system been restored to its original state? □

HAS THE INCIDENT BEEN RECOVERED FROM?

- Has data been restored from backups? □
- Have systems and networks been reconfigured? □
- Have employees been trained on new security procedures? □

HAS THE INCIDENT BEEN INVESTIGATED?

⚠ How did the incident happen? .... □

⚠ What was the root cause of the incident? .... □

⚠ What plan has been developed to prevent future incidents? .... □

HAS COMMUNICATION WITH STAKEHOLDERS TAKEN PLACE?

⚠ Have stakeholders been kept informed of the incident and the response? .... □

⚠ Have updates been provided on the progress of the investigation and remediation? .... □

⚠ Have the lessons learned from the incident been communicated? .... □