Incident Response

Service Definition Document

January 2026

Document Control

Document Type	Confidential - Customer Facing		
Company	Maple Networks		
Address	The Print Rooms 164/180 Union Street London SE1 0LH		
Primary Contact	Graham Tetley	**Role**	CTO/Lead Consultant
Phone Number	020 3858 0048	**Email address**	gtetley@maplenetworks.co.uk

Revision History

Issue Date	Author	Version	Revision Description
12/01/2026	Rory Leanord	0.1	Initial Draft
27/01/2026	Graham Tetley	1.0	QA and Release

Table of Contents

Contents

Services Overview

Maple Networks are next generation Digital and IT service provider in the UK with skills in various areas across the digital landscape. Maple Networks have developed a range of services to support customers in their digital, data and business transformations.

This Document provides overview service definition information for the Maple Networks Incident Response service (IRs).

Maple IRs service delivers a structured and methodical approach, leveraging best practices and industry standards to address a wide variety of cyber threats and incidents. With a dedicated team of experts, Maple Networks supports clients throughout the entire incident lifecycle, from initial detection and analysis to recovery and post-incident review. This ensures that our clients are well-prepared, resilient, and able to respond effectively to evolving cyber risks.

Service Description
Incident Response

Incident Response (IR) is a critical component of any organisation's cybersecurity strategy. In today's digital landscape, cyber threats are increasingly sophisticated and can cause significant disruption, monetary loss, reputational damage, and legal consequences if not managed effectively. Maples robust CREST accredited, NCSC assured Incident Response service enables organisations to quickly detect, contain, and remediate security incidents, minimising their impact and supporting a swift return to normal operations.

By having a dedicated CREST accredited IR process in place, organisations not only enhance their resilience to cyber-attacks but also demonstrate a proactive commitment to protecting sensitive data, stakeholders, and business continuity.

Service Overview

With a dedicated team of cybersecurity experts, Maple Networks leverages industry best practices and proven methodologies to help clients prepare for, respond to, and recover from a wide variety of cyber incidents. Our IR service covers the full incident lifecycle, offering tailored support to stakeholders at all levels.

- CREST Accredited
- NCSC Assured
- Rapid incident analysis and assessment
- Remediation guidance and support
- Forensic investigation of security events
- Communication and coordination with executive and technical teams
- Post-incident review and reporting
- Recommendations for process and security improvements
- Support for legal and regulatory compliance
- Training and awareness for staff and stakeholders

By choosing Maple Networks' CREST Accredited IR service, organisations demonstrate a proactive commitment to cybersecurity, ensuring that sensitive data, stakeholders, and business operations are protected against ever-evolving cyber threats.

Maple have extensive experience across a wide range of organisation types and structures. Across all sectors, Maple have a considerable number of examples of delivering similar engagements at different stakeholder levels. Maple aligns our reports and presentations to executive level, as well as to Senior Leadership Teams and Technical staff. Maple's skills at a technical level across multiple platforms and technologies, include:

- Hybrid multi-cloud
- Backup
- Cyber security
- Disaster Recovery
- Business Continuity

This expertise means Maple are well positioned to deliver on such engagements by leveraging all of our accrued experience and knowledge. Maple have developed a proven methodology which has delivered defined outcomes for our customers.

Maple's proven methodology has been developed over several years, leading to successful delivery of large-

scale reviews, roadmaps, and implementation projects for many commercial organisations including within the NHS, local government, and higher education.

Service Package

Objective	Provide rapid high quality incident response capabilities for customers by highly skilled and experienced technical experts.
Description	Maple Networks' CREST Accredited Incident Response (IR) service provides organisations with a comprehensive, structured approach to managing and mitigating cybersecurity incidents. Our service is designed to ensure rapid detection, containment, and resolution of security threats, supporting business continuity and minimising operational, financial, and reputational impact.
Supported From	All support and management are delivered remotely from Maple's 24x7x365 SOC & NOC
Support level	The service includes the following support levels on the platform: • Remediation support The level of support per customer will be customised and specific to each individual customer.
Required connection types	The service requires internet connectivity. Maple will establish a remote session to customer environments by a pre-determined method suitable for both parties.

Service Features

	Description	Standard / Optional / Customisations
Rapid incident analysis and assessment	Maple's CREST IR provides immediate evaluation of security incidents to determine scope, severity, and potential impact. Leveraging industry best practices and automated detection tools, the service enables organisations to quickly identify root causes, assess affected systems, and prioritise remediation actions. The process includes:	Standard
Remediation guidance and support	Maple's CREST IR provides expert-driven recommendations and hands-on assistance to contain, eradicate, and recover from security incidents. This includes step-by-step guidance for system restoration, patching vulnerabilities, and implementing preventive measures to ensure business continuity.	Standard
Forensic investigation of security events	Delivers in-depth analysis of compromised systems and data to identify attack vectors, timeline of events, and threat actor behaviour. Utilises advanced forensic tools and methodologies to preserve evidence for internal review and potential legal proceedings.	Standard
Communication and coordination with executive and technical teams	Maple's CREST IR ensures clear, timely, and structured communication during incidents. Ensures alignment between leadership and technical teams through status updates, decision-making support, and escalation management to maintain transparency and confidence.	Standard
Post-incident review and reporting	Maple will conduct a comprehensive review of the incident lifecycle, documenting findings, actions taken, and lessons learned. Provides detailed reports for stakeholders, including executive summaries and technical deep dives, to inform future risk mitigation strategies.	Standard
Recommendations for process and security improvements	Maple will offer actionable insights to strengthen organisational security posture. Includes process optimisation, technology enhancements, and policy updates based on incident analysis and industry best practices.	Standard
Support for legal and regulatory compliance	Maple ensures incident response activities adhere to relevant laws, regulations, and contractual obligations. Provides guidance on reporting requirements, evidence handling, and collaboration with legal counsel to minimise compliance risk.	Standard
Training and awareness for staff and stakeholders	Maple delivers tailored education programs to improve security awareness and incident readiness. Includes workshops, simulations, and best-practice guidance to empower employees and stakeholders in preventing and responding to threats effectively. This will be done in lieu of retainer usage.	Standard

Supporting services

Maple Networks Service Desk	• Provides 24x7x365 support and management of the service and supporting infrastructure • Handles events, requests, queries, and incidents raised by authorised users only, whether by phone, e-mail, or self-service support portal • Resolves problems with, applies changes to, and maintains the patch state of, the service platform in accordance with Maple Networks' change management process • Makes configuration changes on request (for example, changes to in scope infrastructure).
Maple Networks Self Service support portal	Maple Networks will provide customer-nominated administrators with access to a Self-service support portal through which they can: • Request additional log sources to be configured • Create new and update existing incidents for investigation • Create new and update existing changes from a change catalogue • See additional services that can be onboarded

Available Service Levels

This chapter identifies the service level measures applicable to the service.

Customers should consider these measures in the context of the general terms and conditions described in full in the Maple Networks Service Level Agreement document (available on request).

Response time	• Incidents
	  ○ P1
	  ○ P2
	  ○ P3
	  ○ P4