INCIDENT RESPONSE WORKFLOW

TECHNICAL

PREPARE

Refer to Pre-Incident Checklist

DETECT

Incident Reported

Monitor Detection Channels

Categorise Incident according to Severity Matrix

User Reports
Automated AV alerts
Email Filters
End-Point devices or servers

Report to ICO

Inform Legal

Report to Action Fraud

Inform Other Stakeholders (External Support)

Contact Details to be defined in supporting documentation and held offline along with this chart

DIAGNOSE

Considerations

Isolate system from network but maintain state

Remove users access privileges

Isolate connections to external partner networks

Obtain and preserve logs. Make a working copy for analysis

Log all actions taken

Identify sources of evidence

IP Addresses, Hostname, MAC Address, Ports, Protocols, Date & Time

Internal and external messaging

Identify systems, services and hosts affected

RAM, HDD, Application Data, Servers, Logs, Meta Data, Active Directory.

RESOLVE

Address the Symptoms and root cause

Ensure impacted services are accessible again

Continue to monitor notification channels

Learn

Review decisions made. What could have been done better? Make improvement to IR plan