**Appendix 2: Incident Management Procedure**

# Incident Response Approach

Incidents are dealt with by cross-functional incident response teams, which involve the most relevant experts for prompt resolution.

The eHealth Service Desks acts as a hub for the coordination and communication of incidents and then escalating the incident as relevant e.g. minor, major or security incidents.

# Preventing Incidents

Since the NHS Fife provides a public service using public resources, it is the responsibility of everyone with direct or indirect contact with eHealth systems or infrastructures to minimise the likelihood of eHealth incidents and their impact.

Prevention of eHealth incidents is the main target of the NHS Fife Information Security Management System (ISMS). It is expected that effective implementation of the eHealth policies will support this strategy e.g. eHealth Change Management, eHealth Information Security, Confidentiality etc.

# The Incident Management Process

The operational system and application of this policy is detailed in the eHealth Incident and Major Incident Management Procedure. The latest version of which can be located on NHS Fife’s Intranet. The link to this document can be found at the end of this policy.

The current incident management system is designed to limit the potential disruption caused by unforeseen events, followed by a return to business as usual, followed by post-incident analysis where it is determined why the incident happened despite precautions and controls.

# Reporting incidents

All users of any of the NHS Fife eHealth systems or infrastructure are required to exercise responsibility in the reporting of eHealth incidents and weaknesses to the eHealth Service Desk when they are encountered.

# Registration / Recording

Any individual providing eHealth first line support to any of the NHS Fife eHealth systems or infrastructures has the responsibility to ensure all reported incidents are registered in the eHealth Service Management system. The eHealth Service Desk will record any reported incidents. External contractors have equivalent obligation to communicate any known or suspected incidents to the eHealth Service Desk.

# Categorisation and Prioritisation

Incidents will be categorised by seriousness, impact, SLA and type e.g. security. The priority of the incident will depend on the category assigned and best use of the support resources available in order to ensure the minimal possible impact to healthcare.

The initial categorisation and prioritisation will be performed by the eHealth Service Desk at the point of registration/recording (or the equivalent first line support engineers – e.g. decentralised system administrators).

It is the responsibility of everyone who detects changes in the impact or seriousness of an incident to report the new situation to the eHealth Service Desk and to ensure it is accordingly recorded and escalated in the eHealth Service Management System.

Major incidents have to be escalated and dealt with according to the eHealth Incident Management Procedure in order to ensure speed resolution, appropriate communications and minimal disruption to the organisation.

# Security Incidents

Security incidents have to be classified as such and escalated to the eHealth Security Manager who will perform this task.

A Security Incident is an actual or suspected event or activity which has, or which might compromise the security of NHS Fife eHealth infrastructure, systems or its data. An information security event indicates that an information security policy may have been violated or a safeguard may have failed, e.g. disclosure or exposure of confidential information to an unauthorised recipient.

Where an incident does not come under the jurisdiction of the eHealth Department, it should be recorded on the Datix Web system, i.e. criminal activity, health & safety, disclosure of confidential data etc.

# Diagnosis and Escalation

The initial diagnosis is typically performed by the eHealth Service Desk or equivalent competent local/de-centralised first lines support staff (e.g. departmental system administrators). They will identify the symptoms of the incident by using standard scripting methods where possible. Where computers/servers are identified as being compromised, the device shall be removed from the network (wired or Wi-Fi) and powered down and collected by an eHealth engineer.

The Service Desk will attempt to resolve the incident at first point of contact. Where this is not feasible; the incident will be escalated to the most appropriate team, internal or external, according to the eHealth Incident Management Procedure for further diagnosis and resolution.

# Resolution and recovery

Once the solution is found, temporary or permanent, the incident will be resolved by the most appropriate team (including third party contractors) following the eHealth Incident and Major Incident Management Procedure.

# Unknown causes of incidents

Those incidents with unknown causes, even if a workaround is found, will be recorded following the eHealth Incident and Major Incident Management Procedure for further investigation and development of appropriate knowledge.

# Incident closure

The person resolving the incident is responsible for closing the call in the eHealth Service Management system as soon as possible, whilst providing all the relevant information to build and share knowledge regarding the resolution, ensuring users are aware the incident is resolved and any competent instructions or guidelines, associated changes in configurations or eHealth assets are adequately recorded, even if it is done as part of a temporary workaround.

SLAs will be recorded based on the time engineers close the call for an incident.

It is the responsibility of the eHealth Service Desk to verify incidents are closed to the user/business satisfaction prior to final closure of the incident.

# Major Incidents – Post Incident Review and Reporting

Once a major incident has been effectively managed and closed, the eHealth Security Manager will document the event in the next Information Security Incident Report. Depending on the type of incident this event may be reported to the I.T. Security Consultant at NISG or to the Scottish Government eHealth Security Officer.

The procedure is covered in the Significant Incident Reporting Guidance eHealth July 2014 document.

The report will be discussed at the next Information Security and Governance Group and where applicable provide recommendations and/or issue actions. These review meetings which take place quarterly as part of NHS Fife’s operational function.