CASTLEREAGH MACQUARIE COUNTY COUNCIL
WEED CONTROL

Information Security Event Assessment Procedure

Contents

1 Introduction

An information security event is an occurrence that may indicate that an incident has occurred or is in progress. Effectively, events are clues that need to be assessed to decide if they need further investigation. Most events will probably not result in an incident being raised.

An event is commonly defined as "any change of state that has significance for the management of information security".

Examples are:

- Notification of a change of an admin password
- Login and logout information at an unusual time
- An unrecognized device having joined the network
- Poor performance of a website
- A device detected as being down when it should be up
- A threshold is breached (or nears being breached), for example disk space capacity
- Messages from security software, for example host-based intrusion detection systems (HIDS)
- SNMP traps from network devices
- Unauthorised logon attempts to key servers or domains
- Failover devices becoming active

It is important that events are recognised as potential incidents so that no such clues are missed. Events can occur from many sources, both automated and human and can be of many different types. Often events are captured in logs which are then reviewed to spot any areas for further attention.

This document provides guidelines concerning how information security events are recognized within Castlereagh Macquarie County Council and a decision made about whether they should be considered to be incidents and managed accordingly.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Castlereagh Macquarie County Council systems.

The following policies and procedures are relevant to this document:

- *Information Security Incident Response Procedure*

2 Information security event management principles

In general, the following principles will be adopted regarding the management and assessment of information security events:

- The approach taken to information security event management should be to ensure that business critical services are addressed first
- Event management will attempt to detect potential information security incidents before they occur and prompt appropriate action to be taken so that they are avoided
- The management of events should be centralized as far as possible so that consistency can be achieved in their processing
- Events should be classified as informational, warning or exception and processed according to their classification
- Events that require action to be taken will be logged as incidents and handled according to the information security incident management procedure
- Responses to events will be automated where possible to reduce the need for human intervention and minimize support requirements and cost
- All events will be logged and retained in accordance with the relevant record retention Policy
- Where possible, appropriate responses to events should be defined in advance and documented. This documentation should be available to support staff at all appropriate times, including out of hours
- Appropriate filtering should be put in place as close to the source of event generation as possible so that events that do not require attention are suppressed and do not use up network capacity
- Where practical, a single event processing engine will be used which is integrated with the incident management system

Events will occur continuously on most types of devices and software. The process of event management is intended to determine which of these require attention and then to route the event appropriately. Events will be detected via a variety of means, including local software running on the affected device (such as Windows event logging) and remote software monitoring devices for certain conditions (for example network intrusion detection systems). They may also be recognized by people, including employees, suppliers and customers.

Once an event has been detected it may be assessed automatically by software according to pre-set rules to determine whether it is informational, a warning or an exception. This assessment may take place on a variety of technical platforms in a range of locations (that is to say it is not necessarily centralised). Informational events will be filtered out but may be kept for later analysis. Warning events will be assessed to see if an automated response is required, or it needs to be brought to the attention of a technical analyst or operator.

Exception events may be escalated from the detecting agent and handled as an incident.

In some cases (particularly for more significant events) the event will then be reviewed to ensure that the correct action has been taken and, if so, it will be closed.

This is a general process which will vary widely in its implementation according to the types of devices and software platforms from which events will be generated, however the principles will remain the same. Where possible, monitoring will be localised in order to make use of specialised software appropriate to that device and to minimise network traffic.

In all cases, attention will need to be paid initially and on an ongoing basis to fine tune the suppression, routing and automation of events on the various platforms so that a useful balance is achieved between maintaining information security and avoiding excessive support requirements.

Events recognised by people may be reported to the IT service desk and logged accordingly for review by the information security team.

3 Procedure for assessing information security events

The following procedures describes how information security events arise and how they are assessed, either automatically or manually to determine whether they should be treated as incidents.

3.1 Event occurs

Events will occur in all areas of our infrastructure and applications and may affect the confidentiality, integrity and availability of many services. Castlereagh Macquarie County Council has a wide range of technology platforms, networks and systems (including physical and cloud-based) from many vendors, each of which has its own techniques and conventions for generating events related to information security.

Effective planning and design will help to reduce the number of exception and warning events that are generated, and informational events will be restricted to those that assist in the management of information security. Excessive generation of events that are not required for warning, exception or audit purposes will be avoided and systems configured as such.

3.2 Event notification and detection

Once an automated event has occurred it will be communicated to the associated monitoring software. In some cases, this will be a module within the system that has generated the event, or it may be an agent running on the same platform or a remote monitoring tool that performs information security “health checks” on a regular basis.

Events may also be notified manually by the users of IT systems or other interested parties.

3.3 Event logged

The event will be logged in order to act as an original record of the event that occurred. This may take place in several places, for example where an event is logged on a local system and then the record is also forwarded to a central monitoring point. This is particularly relevant in security breach situations where the remote log may be taken as more trustworthy than the original which is on the compromised system.

Manually reported events may also be logged in the service desk system.

3.4 First-level event correlation and filtering

The event will then be assessed to determine its type, which may be one of:

- Informational – no action is necessary
- Warning – action may be required soon, or now in order to prevent an exception
- Exception – action is required to address an out of line situation

This assessment may be carried out automatically in several locations according to the way in which the component generating the event is monitored. For components that have built in event logging the first-level event correlation will take place on the device itself. For devices monitored remotely it is likely to happen on the remote monitoring system.

Where possible, events generated automatically will give a standard indication of their severity, that is whether they are informational, warnings or exceptions. This standard will be defined and used in all areas in which messages can be tailored to comply with it and will include:

- Message type – informational, warning, exception
- Impact and Urgency of the event
- Event description in terms understandable by the intended recipient
- Normal resolution actions if appropriate
- Escalation information

3.5 Informational events

Informational events will be automatically closed (although this may not involve any explicit action) and kept for a period of time according to the record retention Policy. Although not forwarded, informational events may still be required for operational purposes to provide an audit trail as part of later investigations.

3.6 Warning events

Those events that are classified as warnings will be subject to further review. Ideally this will be automated via a correlation engine, but this may also be a manual activity carried out by operations staff.

If it is determined that no further action is required at the time, the event will be closed. For those events that need action to be taken, an automated response may be triggered by the correlation engine, for example to increase table size in a database. If an automated response is not possible then a member of the support team will need to decide about what to do next. The information contained in the event message may help in deciding this.

If appropriate, the warning message may be automatically escalated to support staff. This may often be the case if the event occurs outside of normal support hours when an on-call person may need to be emailed, paged, or contacted via some other means. The individual contacted will then decide upon further action to be taken.

3.7 Exception events

For events that are deemed to be exceptions, an incident will be raised, and the event will then be managed via the information security incident management procedure with appropriate diagnosis, investigation and escalation. This may be done automatically or manually.

Key considerations in deciding whether an event represents an incident will include situations where:

- There is evidence of deliberate human interaction for malicious purposes
- The information involved is of a high classification level
- The circumstances are unusual in some way
- There is a clear breach of information security Policy
- There is obvious potential for the situation to worsen if not addressed
- The actual or potential impact on the organisation is significant
- There is evidence of a control not working effectively
- A set of behaviours known to be malicious is displayed
- There is any other reason to be suspicious

If there is doubt about whether an information security incident should be raised, employees should err on the side of caution. Such situations should then be reviewed after the completion of investigations to decide whether similar events in the future should be raised as incidents.

3.8 Review actions

For those events that are more significant (for example because they have a bigger impact on services) a review will be undertaken to ensure that the process has worked effectively and that all required actions have been taken. If this is found not to be the case, a repeat of earlier activities in the procedure may be needed.

3.9 Close event

If the event has been handled satisfactorily it is then closed. Exception events that result in an incident being raised will be subject to the incident management procedure and may be closed under the control of that procedure.

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES