



## **First Responders' Guide: Template**

This document is provided to assist IT security officers in recording the procedures used in their organisation to respond to electronic attacks on their systems. It should be read alongside 'First Responders' Guide; Policy and Principles'.

(This page is intentionally blank)

# Contents

Contents .....	3
Introduction .....	5
How to use this document.....	5
Preparation .....	5
Detection.....	9
Containment .....	15
Eradication .....	17
Recovery.....	18
Lessons learnt .....	19
Appendix A: Checklist of procedures .....	21

(This page is intentionally blank)

## **Introduction**

---

This document forms a template for recording the procedures used by organisations in response to electronic attacks on their systems. The template is arranged according to the policy statements in “First Responders’ Guide: Policy and Principles”. Examples and procedures for each policy are provided.

## **How to use this document**

---

IT Security Officers should use the examples given as an aid to documenting their procedures. The examples should be removed in completed versions of the procedures. For each policy statement the procedures should be referenced, incorporating any procedures identified in this document under the policy statement.

## **Preparation**

---

- 1. Organisations should have policies to assess the risk of electronic attack on their IT systems, including the business impact of attacks, and should identify and implement countermeasures to reduce the risk of attack to an acceptable level.**

### **Examples**

- Accreditation Document Set (UK central government)
- Organisational security policy
- System security policy
- Domain security policy
- IT security procedures

### **Procedures**

The organisation should have IT security procedures that comply with the IT security policy. Details of these procedures are beyond the scope of this document. UK central government departments and agencies should see HMG Infosec Standard No. 2 ‘Accreditation Documents’ under ‘SyOPs’. UK central government also has a risk management framework for IT security defined in Infosec Standard No. 1 ‘Residual Risk Assessment Method’. A reference to organisation security procedures can be added here.

- 2. Organisations should support a management structure that allows risks associated with electronic attack to be mitigated and a response to be made to any incidents reported.**

## Examples

- Senior Information Risk Owner (SIRO) for UK government agencies and departments.
- Senior executive reporting to board, dedicated security team.
- Senior executive reporting to board, part time security team.
- Responsibilities of managed service providers to support incident response.

## Procedures

The organisation should document its internal structure, including internal reporting and accountability channels. A reference can be added here if it is not documented in the organisational security policy.

### **3. Organisations should have an incident response capability or team with policies and operating procedures that are defined by higher management.**

## Examples

- Senior executive reporting to board, dedicated incident response team.
- Senior executive reporting to board, part time response staff (corporate security personnel, system security officers, system administrators).
- Managed service providers provide incident response team.
- Managed service providers provide detection support to organisation incident response team.

## Procedures

The operating procedures for the incident response team are defined by completing this document. There are some specific procedures which should be included.

- Procedures for regularly testing incident response via table top and operational trials.
- Procedures for personnel security matters insofar as they affect electronic attack:
  - interviewing procedures;
  - disciplinary procedures; and
  - HR policy and personnel handbook.

- 4. Organisations should have a contact list for members of the incident response team, for incident response teams of organisations that provide managed services to them, and a point of contact for the team.**

#### **Examples**

- Telephone numbers, pager numbers and email addresses for incident team members.
- Telephone numbers, pager numbers and email addresses for the incident response teams of managed service providers.
- Group telephone number, pager number and email address for incident response team.
- Home numbers should be included if the response team provides out of hours response.

#### **Procedures**

The incident response team should maintain a team contact number and provide details of hours of operation. The incident response team should maintain a list of contact details of members of the response team, and should test the communications mechanisms on a periodic basis to ensure that they are effective.

- 5. Organisations should have a plan for business recovery which should be practiced regularly.**

#### **Examples**

- Plan and procedures for backup and recovery of business data.
- Plan and procedures for rebuilding a system to a standard organisational specification (but with the latest relevant security updates).
- Exercise plan to test business recovery.
- Provision of physically redundant connectivity between sites.
- Provision for redundancy in service provision (“hot” or “cold” standby).

#### **Procedures**

Business recovery procedures should be referenced here.

**6. Organisations should actively monitor for new vulnerabilities and exploits that could affect their systems.**

**Examples**

- Identifying products used in systems ('IT inventory').
- Identifying network topology and points of access (which may be confirmed during penetration testing).
- Monitoring vendor web sites.
- Monitoring vulnerability web sites.
- Subscribing to vulnerability mailing lists.
- Having penetration testing and vulnerability scanning performed against systems.

**Procedures**

Keep a list of the products that are used on your IT systems. Actively monitor for vulnerabilities using web sites and vulnerability mailing lists (including UNIRAS alerts and briefings). Periodically check your systems for vulnerabilities using vulnerability scanners and using qualified penetration test teams.

**7. The incident response team should have a way of assigning and managing priorities in responding to incidents and a procedure for escalating the incident in order to engage business management.**

**Examples**

- Qualitative priority assignment based on risk to the business (low, medium, high), (minor, major, critical).
- Quantitative priority assignment (one to five for example).

**Procedures**

Identify priorities based on risk to the business (see NISCC Technical Note 04/04, available from <http://www.niscc.gov.uk/niscc/docs/re-20040325-00157.pdf> ). Assign greater resources to high priority incidents and a shorter deadline for resolving the incident. In the event that the priority represents a high risk to the business, notify the management of the incident response team in the organisational context, who will then be responsible for managing the impact on the business.

**8. The incident response team should have a system to record all actions taken in respect of an incident and store that information for later retrieval.**

**Examples**

- Use of an incident tracking system.

- Use of helpdesk software.
- Use of a bug tracking system.
- Use of a paper based journal system.

## Procedures

All actions taken in respect of the incident should be recorded in an incident journal (electronic or paper based).

The following should be recorded:

- Time and date of incident;
- Who or what reported the incident;
- Incident description; and
- What is affected by the incident.

9. **All incident response teams should have the capability to gather evidence of the cause of an incident in such a way that it does not interfere with investigations by NISCC, national security or law enforcement authorities.**

## Examples

- Annotating all actions and results obtained.
- Mounting the affected device read only so that its contents are not altered by the actions of the investigator.
- Sealing evidence collected in bags with tamper evident seals where it is retrieved for subsequent analysis.

## Procedures

Please reference forensics procedures here. Contact NISCC Response for on-site forensics support if your organisation does not have a developed forensics capability.

## Detection

---

10. **All organisations in the NISCC constituency should, at minimum, follow best current practice in the detection of IT security incidents.**

## Examples

- Logging by firewalls, operating systems and application
- Configuring alerting on security events in the logs
- File integrity checkers
- Intrusion detection systems (host based and network based)
- Anti-virus measures
- Anti-spam measures

- Email and web content checkers

## **Procedures**

Current best practices should be identified and architectures introduced that implement those practices. Where applicable, NISCC and, for UK central government, HMG information security guidance should followed. The best current practices as used in the organisation should be documented. Best current practices should be referenced here.

### **11.The incident response team should investigate any incident or anomalous occurrence reported to it.**

#### **Examples**

- New, unexpected user accounts have been found on the system
- New, unexpected files have been found on the system
- Unexpected network activity has been detected
- There are unexpected gaps in the logs
- The system performance has degraded significantly
- A security application issues an alert
- A web site belonging to the organisation is defaced
- Suspicious emails are received

## **Procedures**

The procedures are itemised in other sections. See policy statements no 9 and 12 *et seq* for example.

### **12.The incident response manager should appoint an incident handler to manage all actions taken in respect of the incident.**

#### **Examples**

- The incident handler could be a member of the full time incident response team
- The incident handler could be a member of the security or operational IT staff

## **Procedures**

The incident handler should open the incident, keep a log of events. They should also be responsible for incident resolution and for monitoring progress towards that resolution.

**13. The incident handler should keep a detailed log of all actions taken in responding to the incident, including time stamps**

**Examples**

- When did the incident happen?
- How long did it last?
- What were the observable effects?
- What is the scope of the incident?
- What locations/systems were affected?
- What was the cause of the incident?
- What actions were taken and when?

**Procedures**

The incident handler should try to establish answers to the questions in the 'examples' from the reporter and should note these answers in the incident journal system. All actions should be noted as the investigation continues.

**14. The incident handler should determine the extent of the incident.**

**Examples**

- Is one standalone computer affected?
- Is a network segment affected?
- Is the local area network affected?
- Is a wide area network affected?

**Procedures**

The purpose of identifying the extent is to identify how easily the incident can be contained and whether to escalate the issue to business management. An incident that affects the whole organisational network should be escalated to business management. The incident handler need only make a broad assessment of impact (but see the next step below).

**15. The incident response team should identify the hosts affected by the incident (for example by unusual or malicious network or host activity) and the source of the incident.**

**Examples**

- Network traffic from a compromised host.
- A device on the network that is receiving larger than normal amounts of data.
- A firewall that is being scanned by an external host.

**Procedures**

The purpose of identifying the hosts affected is to confirm the accuracy of the incident report. The task is performed by monitoring intrusion alerts and traffic on the network or by viewing the logs on the affected host. The same techniques can be used to identify the source of the incident, which is particularly significant if the source is a host on the internal network.

**16. The incident handler should determine whether the incident report is a false alarm.**

**Examples:**

- Is the report relevant to the system?
- Is the issue a security issue rather than a performance issue?
- Does the report relate to normal system behaviour?

**Procedures**

Hosts and networks should be analysed for evidence of the incident having occurred. If no evidence is found then the incident can be closed.

**17. The incident handler should attempt to determine the type of incident.**

**Examples**

- Port scanning
- Denial of service
- Successful hacking attack
- Blocked hacking attack
- Successful virus/worm/malicious software compromise
- Data interception and monitoring
- Breach of corporate security policy

**Procedures**

The observed effects of the incident should be used to assist in the identification of the incident. It may be difficult to distinguish a malicious software compromise from a successful hacking attack. In that case the incident type should be left open until further investigative steps have been taken (see below).

**18.If the incident is not a denial of service from an external source, the incident handler should determine whether the incident report relates to an unsuccessful attack or to a system compromise.**

### **Examples**

- Anti-virus alarm (unsuccessful attack)
- Blocked firewall entries (unsuccessful attack)
- Attempts to exploit a non-vulnerable product (unsuccessful attack)
- Evidence of services/applications restarting at random (system compromise)
- New, unexpected user accounts have been found on the system (system compromise)
- New, unexpected files have been found on the system (system compromise)
- There are unexpected gaps in the logs (system compromise)
- There are unexpected network connections originating from your network (system compromise)

### **Procedures**

The incident handler should use the examples to determine whether the attack relates to a system compromise or to an unsuccessful attack. The incident handler should assign a lower priority to an unsuccessful attack than to a successful attack.

**19.The incident handler should assign a priority to the incident in consultation with business management.**

### **Examples**

- An incident affecting large parts of the organisation's networks or hosts should be assigned a high priority.
- An incident affecting a host which is critical for business operation should be assigned a high priority.
- An incident which involves possible data exfiltration from a host containing sensitive data should be assigned a high priority.
- An unsuccessful attack should be assigned, at most, medium priority.

### **Procedures**

The incident handler should escalate all high priority incidents so that business management can take business decisions based on risk to the business. The 'examples' should be used as the basis for making decisions on priorities.

**20. If a successful attack, the incident handler should report the incident to the NISCC Response team.**

### **Examples**

See clause 18

### **Procedures**

Details are provided at <http://www.niscc.gov.uk/niscc/reportIncident-en.html>.

**21. The incident handler should ask the reporter whether the incident should be passed to the police for investigation.**

### **Examples**

- Has the computer been subject to unauthorised access?
- Has data on the computer been subject to unauthorised modification?
- Has the computer or data on the computer been permanently damaged?
- Has there been any attempt at blackmail or extortion?

### **Procedures**

Incidents can be reported to NISCC in the first instance, which will pass the information to the police if requested. The incident handler should make clear that there is a belief that criminal activity has taken place.

**22. If the incident is a hacking attack or targeted malicious software, the incident response team should take a digital image of the computers' hard disks.**

### **Examples**

- No action taken by the response team should change data held on a computer or storage media, subject to the following proviso
- In exceptional circumstances where it is necessary to access live systems (for example, to capture volatile data), the investigator should be competent and able to give evidence explaining the relevance and the implications of their actions
- Other technical staff should be made aware of the need to preserve computer evidence, and advised to seek help from a trained investigator at the earliest opportunity
- An audit trail or other record of all processes applied to electronic evidence should be created and preserved
- This chain of evidence should be maintained in respect of media and documentation. Records should account for the storage and handling of all material at all times. The use of tamper-evident bags and secure storage facilities is desirable

- The settings of any inbuilt clocks should be recorded, so that accurate statements can be made about the timing of events
- Media which will hold copies of original material should be reinitialized to a known state before use, to avoid contamination of evidence with pre-existing data
- Digital images should be generated using forensically sound methods. Commercial and open-source software tools are available for this purpose

## Procedures

It is important to ensure *in advance of any incident* that your organisation has a proper policy framework to support such investigative work – and in particular that it takes into account legislation on individual privacy.

The example guidance above should be followed. If in any doubt, please contact NISCC Response for advice and on-site assistance.

**23. If the incident is a hacking attack or targeted malicious software, the incident response team should perform network forensics on the computers affected and capture the state of running processes**

## Examples

- Passively monitor traffic to/from the affected system(s).
- Determine whether it is appropriate to image system prior to carrying out network forensics, balancing the need to capture volatile data against the possibility of changing the content of the target system. If appropriate, then:
  - work from write-protected media containing trusted copies of software tools;
  - document the current state of network sockets on the affected machine(s);
  - identify which processes are bound to each socket;
  - dump the memory associated with running processes; and
  - Perform a remote enumeration of the services running on affected machine(s).

## Procedures

The example guidance above should be followed. Prior preparation - identifying reliable tools, burning them to CD-ROM, and training staff in their use – is very important. If in any doubt, please contact NISCC Response for advice and on-site assistance.

## Containment

---

**24. The incident response team should isolate (for example, physically disconnect from the network) any computer or networked device that**

**is believed to be compromised by malicious software or a hacking attack.**

### **Examples**

- A computer infected with a virus or worm
- A router that has been compromised
- A firewall that has been compromised

### **Procedures**

Once any hosts affected have been identified and forensic activity undertaken, the incident response team should disconnect affected hosts from the network (if they are networked). The incident response team should note the identity of the host (IP address, name and serial number).

**25. If a computer or networked device cannot be isolated individually, the incident response team should isolate the local area network to which it is connected.**

### **Examples**

- All hosts in a local area network have been infected with an internet worm
- All hosts in a local area network are vulnerable to a vulnerability used in a compromise of a particular host

### **Procedures**

The routers and firewalls at the boundary of the network should be configured to deny all traffic, inbound and outbound. The changes to the network configuration should be noted, for later restoration.

**26. The incident response team should keep system users informed of their actions.**

### **Examples**

- Advice that a system is currently unavailable but is estimated to be back in service at a certain time
- Advice to prevent further incidents such as opening certain emails

### **Procedures**

System administrators should use standard customer relations management process to alert users of the impact of the incident. A reference may be added here. Security awareness advice may be provided if appropriate to the incident.

## **Eradication**

---

**27. The incident handler should identify measures to prevent continuation of the incident.**

### **Examples**

- Change the external IP address/domain name of your gateway (denial of service attacks)
- Run an anti-virus product
- Rebuild compromised computers

### **Procedures**

The incident handler should document the measures identified, which may refer to containment measures.

**28. The incident response team should implement measures to prevent continuation of the incident.**

### **Examples**

See measures identified

### **Procedures**

Changes should be applied to system and network configurations as previously identified. All changes should be recorded and the effects of the changes noted.

**29. The incident response team should rebuild computers and networked devices that are believed to be source of the incident on a separate trusted network to the network that has been compromised.**

### **Examples**

- A computer network that has been infected by a worm
- A computer network that has been compromised by malicious software that can be activated remotely

### **Procedures**

The incident response team should reformat/remove evidence of the compromise of the computers in isolation, but can use a trusted separate network to upload new images to the hosts.

**30. The incident response team should analyse the digital evidence collected and determine the vulnerability exploited (if any) and the origin of the attack.**

### **Examples**

- Identify the patch status of the machine and catalogue installed software
- Construct a time line of file system changes
- Eliminate legitimate files from consideration by comparing with a clean system
- Use hash sets of known malicious software to identify artefacts associated with the attack
- Carry out a keyword search for IP addresses and terms relevant to the investigation

### **Procedures**

The incident response team should document every step in the analysis and record what actions have been performed on the computer. NISCC Response will provide assistance in analysis of the digital evidence.

## **Recovery**

---

**31. Once all eradication and prevention measures have been applied, the computers and networked devices should be retested for the presence of the original vulnerability.**

### **Examples**

- Run anti-virus scan on affected hosts
- Run vulnerability scan on compromised hosts
- Check that all patches and updates have been applied

### **Procedures**

All steps in the testing process should be documented.

**32. Once all eradication and prevention measures have been applied, the computers and networked devices should be tested for evidence that no unexpected or malicious behaviour is exhibited.**

### **Examples**

- Check that the network socket activity is as expected (compare with a known clean host)

- Check that check sums of the main system files (including configuration files) match those on a known clean host where there are not local differences (IP addresses for example)

All steps in the testing process should be documented.

**33. Once all eradication and prevention measures have been applied and the devices have been tested and found to behave normally, the devices may be reconnected to the network and/or returned to their original operational role.**

### Examples

Not applicable

### Procedures

All steps in the testing process should be documented.

## Lessons Learnt

---

**34. The incident handler should write a report on the incident for the organisational security officer including recommendations on any changes in security measures.**

### Examples

- Log entries should be provided in summary and in detail.
- Extent of the incident should be identified.
- Measures taken to remediate the incident should be provided.
- Future prevention measures should be identified.
- Impact of the incident should be assessed.

### Procedures

A standard organisational reporting template should be followed. Insert documentation standards reference here.

**35. The business management need to consider the incident handler's recommendations and should address wider business practices that have been impacted by the incident.**

### Examples

- Blocking executable file types at the organisation gateway.
- Looking at the impact of allowing business computers to be used at home.
- Information sharing with business partners.

## Procedures

Business management should write a report on the business impact of the incident and future revisions to business practices.

**36. The public relations officer should consider if a statement to the media will be needed.**

## Examples

- Does the incident involve outside organisations or individuals?
- Are the police involved?
- Will there be a large financial loss to the organisation?
- Are any individuals in the organisation being targeted?

## Procedures

The organisation's media policy should be referenced here.

**37. The incident handler should close the incident when the incident is no longer active, all alterations to the system associated with the incident have been removed and adequate measures to prevent a repeat of the incident are in place.**

## Examples

- An incident should only be closed if no further action is required by anyone involved in the incident.
- An incident should not be closed if the same incident could happen again to the same system.
- Open incidents should be reviewed at least once a week.

## Procedures

Incident closure for a high priority incident should be agreed with the business management. Closed incidents should be recorded for statistical reporting purposes and for awareness training in the organisation.

## Appendix A: Checklist of Procedures

### Organisational Policies

PROCEDURE NAME	REFERENCE IN DOC	YOUR REFERENCE
Organisational Security Procedures	Clause 1	
Accountability structure	Clause 2	
Incident Response Procedures	Clause 3	This document
Business Recovery Procedures	Clause 5	

### Incident Response Policies

PROCEDURE NAME	REFERENCE IN DOC	YOUR REFERENCE
Vulnerability & exploit monitoring procedures	Clause 6	
IT product inventory	Clause 6	
IT network topology	Clause 6	
Incident prioritisation procedures	Clause 7	
Incident recording procedures	Clause 8	
Computer forensics procedures	Clauses 9, 22, 23	
User impact procedures (including procedures for alerts and warnings)	Clause 26	

(This page is intentionally blank)