BERGRIVIER MUNICIPALITY

INCIDENT HANDLING POLICY

APRIL 2012

INCIDENT HANDLING POLICY

REVISION NUMBER	DATE	AUTHORISED FOR DISTRIBUTION

1. INTRODUCTION

The aim of this policy is to:

- Allow Bergrivier Municipality to keep a record of all faults/problems and systems changes and to document such changes.

- Allow the System Administrator to monitor all computer faults within the departments so that any matters arising can be monitored.

- Allow the respective Department to monitor all requests to vendors.

- Monitor cost to establish if it is still economically viable to repair certain equipment, or to allow management to make decisions to replace equipment that is no longer economically viable to be repaired or outdated and obsolete.

2. POLICY STATEMENT

The following statements describe the incident policy and exclude all financial applications:

- The occurrence of all incidents and change and service requests must be logged with the IT Department on ithelpdesk@bergmun.org.za or (022) 913 6033. This policy covers a new service being required, a problem being experienced or further information being requested.

- No action will be taken or assistance and support provided unless it is logged and a reference number provided. However, in most cases the staff member logging the call will be able to provide the required information or help immediately.

Depending on the nature of the problem or request, there are different procedures to follow when requesting a change, service or information or reporting a fault or a problem. However the policy is that:

- The staff member must report the problem/fault to his or her manager. This can be done verbally, in writing or via e-mail.

- The ICT Department will then attend to the problem and issue a complaint number to enable them to reference the logged problems/faults.

In addition, no staff member may request any work directly from any ICT vendor without first following the above policy.

The vendors have been instructed that any requests attended to without the proper policy and procedure having been followed will not be for the account of Bergrivier Municipality. In cases where a staff member does not follow this procedure, any charge levied by the vendor, will be for the account of the relevant staff member.

3. GENERAL GUIDELINES

During an emergency situation the following guidelines and principles are advised:

- Remain calm – A compromised system is a call to action but not a cause for panic.

- Take good notes – Take detailed, organized and complete notes while handling any computer security incident preferably in an automated manner following a template so that no critical detail is missed especially if it may be required as evidence in the future. The documentation should be time stamped and auditable.

- Notify the right people and get help – Inform those who "need to know" about the incident. Again this should be an automated process.

- Enforce a "need to know" policy – This is one of the hardest things about handling an incident as they can be misdiagnosed early on. It is better therefore to inform those who need to be appraised of the situation so as to manage consistent communication.

- Use out-of-band communications – Whenever possible, use telephones and faxes during a computer security incident. If the attackers have full access to the Help Desks computers and they can read the mail. If the Help Desk's computers are used, this allows the intruder to know when the incident is reported and what response is received.

- Contain the problem – The first time that the compromised computer is touched, it should be to disconnect from the network, even if it is a core infrastructure resource. In order to contain the problem and regain control, all communication between the compromised host and other hosts on the network must be stopped.

- Make backups - Make backups of system information as well as file-system information. Process tables, network connections and other volatile data sources should be dumped to files and then backed up with the rest of the file-system.

- Get rid of the problem – The problem must be completely eradicated. Determine the cause of the incident, then reload a clean operating system and improve the system's defences by installing the appropriate software. Only then can the system be reconnected to the network.

- Get back in business – The goal is to make the recovered system resistant enough so that Bergrivier Municipality has a fair chance of determining that it is under attack before it falls.

4. INCIDENT HANDLING PROCEDURE

The following phases are the constituents of Bergrivier Municipality's incident handling procedure:

4.1 Phase 1 Identification

- Assign a person in the IT Department to be responsible for the incident.

- Determine the extent of the incident utilizing diagnostic tool kits.

- Be careful to maintain a provable chain of custody particularly when it relates to a security incident as the evidence may be required in a court of law. Examples of this could be:
    - Identify every piece of evidence with a witness.
    - Sign, seal and date a copy of everything.
    - Place everything in a tamper-proof locked place that only a very limited number of people have access to (and be able to prove only a limited number of people have access).
    - Sign, seal and date a copy of everything.
- Coordinate with the people who provide your network services as they can proactively block incoming and outgoing traffic and can help trace security violators.
- Notify the appropriate officials.

4.2 Phase 2 Containment

- Deploy IT Department Staff to survey the situation avoiding disruption of normal routines. Task somebody to be "the recording secretary" so that nothing is left to memory.
- Keep a low profile so as to contain the problem and not raise tension at Bergrivier Municipality unnecessarily.
- Back up the system.
- Determine the risk of continuing the operation of the system.
- Continue to consult with the System Owners so that they are informed and will not disrupt the team that is handling the incident.

4.3 Phase 3 Eradication

- Determine the cause and symptoms of the incident.
- Improve defenses.
- Perform vulnerability analysis.
- Remove the cause of the incident.
- Locate the most recent clean backup.

4.4 Phase 4 Recovery

- Restore the system.
- Validate the system.
- Decide when to restore operations when it would have least business impact.
- Monitor the systems.

4.5 Phase 5 Follow-up

- Develop a follow-up report.