Incident Management Procedure

iGRC (Governance, Risk & Compliance)
Effective Date: Aug 01, 2012

RESTRICTED

Contact Details

Document Control

History						
Prepared/Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval	Date of Implementation
[redacted]						

Change From Previous Version
Incident Response Team changed Incident Investigation team Formed The flow of incident escalation has also been revised. IRT Team Revised.

TABLE OF CONTENTS

1 INTRODUCTION

Incident Management is a core process that every employee needs to master. This process helps the community of IT service users to resolve Information Security Incidents that can emerge within different IT structures. Effective and efficient Incident management within the premises of Interactive Group will be beneficial for the operation of uninterrupted business activity.

2 PURPOSE

Incident management identifies, classifies, and manages the resolution of Information Security Incidents while minimizing their impact to the business. This role is critical in ensuring that the impact of incidents (both general and technical) on the business is managed effectively. And it offers the hope that future incidents can be mitigated as incident management programs become more proactive with the passage of time.

3 SCOPE

This procedure governs the [redacted] general response, documentation and reporting of information security incidents affecting information resources in hard or soft form. This procedure does not include damage to personal computers owned by employees or consultants, unless their computers contribute to the Incident with [redacted].

4 PROCEDURE

Security incidents at [redacted] are divided into two domains technical and general. Information Security incidents are defined as single or a series of unwanted or unexpected information security events that have a significant probability of compromising business

4.1 INITIAL REPORTING

All information security incidents, including suspicious events that may result in an incident should be reported immediately to helpdesk (VoIP [redacted]), by the employee who has witnessed/identified an activity (that has already occurred or may occur) resulting in potential disruption in a business activity. A ticket is generated by the helpdesk and a number is assigned to that incident e.g. TI#123 for technical incidents and GI#12 for general incidents.

4.2 ESCALATION

There are two teams for managing the incidents.

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- IRT (Incident response team) for general incidents.

- The members of this team shall be decided by Sr. Manager Facilities & Physical Security.

Information security incident is first escalated to designated members of respective IRT via call on mobile and/or VoIP. An email is floated to the respective aliases i.e. [redacted] for technical incidents and [redacted] for general incidents.

Example of a format Helpdesk shall use to forward the email to IRT members:

Incident Number: TI-25

Incident Location: [redacted]

Incident Reported By: [redacted]

Incident Summary: Loss of data on a critical business machine.

The IRT shall determine if a security incident is indeed underway. If more information is required to analyze the reported incident, IRT may contact the person who initially reported the incident for acquiring more details.

4.3 INVESTIGATION OF TECHNICAL INCIDENTS

Note: General incidents shall be investigated by Sr. Manager Facilities & Physical Security.

1. If IRT decides that an investigation is required for an Information Security Incident, the case is forwarded to the incident investigation team.
2. Technical incidents shall be investigated by the following members:
   - [redacted]
3. Every effort shall be made to save log files and system files that could be used as evidence of a security incident.
4. This includes backing up the affected environment; thoroughly documenting all activities performed on the affected platform or environment to contain, mitigate, and restore the environment; storing any potential evidence, such as drives, diskettes, or tapes, in a locked container; and documenting and controlling the movement and handling of potential evidence in order to maintain a chain of custody.

5. The Information Security Incident investigation team shall serve as the focal point for collection of evidence.

4.4 MITIGATION AND CONTAINMENT OF TECHNICAL INCIDENTS

1. Any system, network, or security engineer, who observes an intruder on [redacted] network or system, shall immediately inform incident response team/helpdesk so that appropriate action can be taken to terminate the intruder's access.
2. The IRT shall decide if the affected systems, (such as those infected with malicious code or systems accessed by an intruder) should be isolated from the network until the extent of the damage can be assessed.
3. The IRT shall quickly eliminate the method of access used by the intruder and any related vulnerabilities. (The detailed steps are outlined in the forensics guideline [redacted])

4.5 ERADICATION AND RESTORATION OF TECHNICAL INCIDENTS

1. The extent of damage must be determined.
2. If the damage is serious and the integrity of the data is questionable, a system shutdown and reloading of operating systems and/or data may be required.
3. Management notification is required if mission critical systems must be taken off line for an extended period of time to perform the restoration.

4.6 INCIDENT REPORT

1. The incident report form is filled by the IRT.
2. If required, evidence is collected and attached to the form in a documented form.
3. Risk levels posed by the incident are identified by the [redacted] department.
4. The sanctions are calculated in coordination with the HR department. This report is then submitted to [redacted] for advice.
5. If the management decides that the identified sanctions are justified and should be allocated to the responsible entity, HR department informs the concerned perpetrator and updates the sanctions allocation record.

4.7 PENALTIES

The responsible personnel identified after the incident investigation will be penalized according to the penalties allocation procedure at [redacted].

4.8 TICKET STATUS

Until the ticket closure email is sent to the helpdesk by an IRT representative a continuous reminder will be generated by the helpdesk for the open incident tickets. Help desk will also be responsible to keep logs of all the reported incidents.

Note: [redacted] will be heading the incident response and will coordinate the investigation of the incidents as per requirements.

5 FLOW CHART