THE CITY OF Red Deer

CORPORATE PROCEDURE

5203-CP

Information Technology Security Incident Plan

Purpose:

1 To establish procedures to handle the abuse of information technologies and security incidents in order to protect users and The City's information technology systems and resources.

Procedure:

2 Information Technology Incident Response Team (ITIRT):

(1) The City's Information Technology Services (ITS) Department will establish an Information Technology Incident Response Team (ITIRT) to respond to information technology security incidents and reports or complaints about the abuse of information technologies. The ITIRT is neither an investigative nor a disciplinary entity in its primary responsibilities.

(2) Members of ITIRT will be selected by the Information Technology Services Manager from within ITS. Team members will include:

(a) Information Technology Services Manager
(b) Information Technology Supervisors
(c) Network Administrator
(d) Production Support Coordinator
(e) Systems Administrators (Technical Analysts)

(3) As deemed appropriate by the ITS Manager, the ITIRT may be expanded to include members from other City departments depending on the specific nature of the incident.

3 ITIRT's Response to Immediate Circumstances, Concerns, and Complaints:

(1) In the case of an incident, the ITIRT will work quickly and collaboratively to establish the nature of the incident and develop an appropriate response that protects the City and reduces the risk of recurrence.

(2) In cases where City resources and privileges are abused or otherwise threatened, the ITIRT will take appropriate short term steps to mitigate risks to The City.

(3) ITS System Administrators, who are members of the ITIRT, are authorized to take the following actions in order to deal with immediate circumstances without prior approval from the ITS Manager:

(a) disable user accounts
(b) interrupt computing processes by shutting down computer systems
(c) disable services such as Internet access or Email services

(4) ITS System Administrators must report the actions taken to the Manager of Information Technology Services who may authorize extending such actions to safeguard City resources.

(5) If the ITIRT decides the best action is to do nothing in order to identify the person(s) responsible for the incident and preserve evidence, the ITIRT shall notify the appropriate Department Head, General Manager or the City Manager.

(6) The reports and findings of the ITIRT are confidential, consistent with this procedure, federal and provincial laws, as well as the rules of the disciplinary bodies involved.

4 Investigations:

(1) Incidents that involve the City's on-line environment sometimes lead to investigations, which include the gathering of technical evidence. These investigations may be activated by law enforcement officers, City managers or by The City's Human Resources Department (depending on the nature of the incident and the role of the person(s) suspected of improper behaviour). In such investigations, investigating officials may call upon the ITIRT to provide technical information from City computers.

(2) Evidence in these investigations may involve computer usage information about individuals which is maintained on centrally-managed computers or individual workstations. Computer usage information about individuals includes two major types:

(a) log information: generally referring to when a user's account was used in various contexts; and

(b) content information: generally referring to content of materials stored in storage space tied to the account as well as "live" content generated or received by a person currently using the account.

(3) The ITIRT is able to provide pertinent log information to investigating officials once they have followed the procedure below for accessing the information. Providing content information such as the contents of a mailbox, a file or a copy of a specific message within a mailbox raises issues of privacy and the Freedom of Information & Privacy Act (FOIP). These requests may therefore require additional review by The City's Access and Privacy Coordinator.

5 Requests for Computer Usage Information:

(1) To obtain computer usage information about individuals, investigating officials will:

(a) Contact the Manager, Information Technology Services at 403-342-8392 or its@reddeer.ca. Requests for access to the specific subtype of computer usage information that involves "content" will require additional review by The City's Access and Privacy Coordinator.

(b) Be as specific as possible in the request, including dates, times, workstations, and usernames. Requests covering narrower time frames can be handled more easily and quickly.

6 Internal Departments:

(a) Managerial staff investigating incidents as part of staff disciplinary processes will need to notify the ITS Manager so advanced discussion can take place about the type of computer-usage information that can be made available.

(b) The ITIRT will not provide log information to managers investigating incidents as part of staff disciplinary processes until approval from the appropriate Department Head and the Human Resources Department is received. Requests for content information will be handled in accordance with relevant FOIP policy.

(c) Unless otherwise instructed in the request, the person(s) whose account(s) were associated with the requested information will be notified that the information was requested and provided, and advise them of the name of the investigating entity.

7 Law Enforcement Agencies or Others Outside the City User Community:

(a) Law enforcement, government officials, and others outside the City community will need to provide legal orders, such as a search warrant, to obtain computer usage information. These documents are to be delivered to: Manager, Information Technology Services City Hall, Floor 4 – IT Services 4914 49th Avenue, Red Deer, AB T4N 3T4

(b) Any such legal documents will be forwarded to other appropriate City officials and to the City Solicitor. The City and its employees will comply with any conditions included in a legal order.

(c) The ITIRT will release computing usage information to law enforcement, or others outside the City user community only after it has been reviewed by the City's Access and Privacy Coordinator and the City Solicitor, unless immediate release of information is mandated by legal order.

(d) Unless otherwise instructed in the legal order, the person(s) whose account(s) were associated with the requested information will be informed that the information was requested and provided, and told the name of the investigating entity.

References/Links:

1 Freedom of Information & Protection of Privacy Act

2 5201-CP Information Technology Usage and Security

Scope/Application:

1 This procedure applies to any employee or contractor with The City who has access to The City's information technology, systems, services, and networks.

Authority/Responsibility to Implement:

1 The Information Technology Services Manager through the General Manager of Corporate Services.

Inquiries/Contact Person:

1 Information Technology Services Manager

Procedure Monitoring and Evaluation

1 This policy will be evaluated every two years with revisions made as required.

THE CITY OF Red Deer

CORPORATE PROCEDURE

5203-CP

Information Technology Security Incident Plan

Approval History:

Date:	Approved/Reviewed By:	Title
Approved: November 29, 2007	"Dan Newton"	ITS Manager
Revised: July 13, 2020	"Allan Seabrooke"	City Manager