



**Corporate Crisis Management Program
Security Incident Response Team Plan
(SIRT)**

**June 2017
Version 1.0**

The SIRT can be activated through the Equifax Notification System or via call tree. Activation should be initiated by SIRT Leader or Alternate.	
Primary SIRT Assembly Point	Fusion Center Conference Room
Secondary SIRT Assembly Point	Bond Conference Room
Conference Bridge Line	Number: 1-866-398-2885 Toll : 1-719-457-1414 Participant Code: Redacted Host Code: Redacted

--	--

Table of Contents

[TOC \o "1 3" \h \z \u]

Security Incident Response Team Plan

During a Response, use the “Action List” beginning on page 15.

Purpose

The Security Incident Response Team (SIRT) defines principles, roles and responsibilities for team members who support the physical, cyber security and life safety aspects of Equifax’s incident response program. This team is known as the SIRT.

This plan is not intended to stand alone; it is used to support the *Equifax Crisis Management Plan* (“CMP”), the Equifax Crisis Management Team (“CMT”) and the Security Incident Handling Policy & Procedures Guide. All SIRT members must be familiar with the details of the CMP.

This plan provides a “Potential Considerations List” for SIRT members and is designed to ensure a consistent, collaborative response during an event by all active SIRTs.

The SIRT Plan is activated by any VP Global Security or above. It will be implemented in context of the *CMP*. The responsibilities of the Security CMT member are listed in *Table A* of the *CMP*.

Security Incident Response Principles

Scope: The SIRT scope is typically limited to the Security Department’s response to an incident that has been declared a security incident by a Security VP or higher. The SIRT Manager and SIRT Coordinator will work in tandem to provide a consolidated incident status for escalation determination.

Focus: The primary focus of the SIRT is on the physical and executive security, information security and personnel safety elements of an incident and on issues that cut across departmental lines. The SIRT will also support or consult with the affected departments and offer specialized resources available at the corporate level.

External Resources: The SIRT may require additional resources beyond those within the company. In all cases of external resources, the resources will be considered part of the SIRT and will operate under the direction of a VP Global Security.

Operational Guidance: The SIRT will use the Potential Considerations List in the SIRT – Action List, beginning on page 16 to manage the Security Department response. Please note that all actions on the list may not be appropriate in every incident, nor are these the only actions required for a successful response. In all cases, judgment should be used to determine the correct actions.





































