Process for Retaining Computing Systems or Storage Drives

During an incident investigation it may be necessary for the IT Security Office to retain computing systems or storage drives for forensic investigation. This hardware retention may be needed to:

- confirm protected information was not accessed,
- help scope the incident,
- retain evidence that might needed for law enforcement investigation,
- gather information for the notification process,
- analyze details about the incident.

Since the retention of hardware may negatively impact the affected department, it is the last resort towards satisfying the incident needs. The determination of whether or not hardware must be retained is made by the TSO. The TSO will contact the IT manager responsible for oversight of the hardware to coordinate pick up. Depending on the urgency of the incident, and availability of the direct manager, the TSO may coordinate the pick up details with other line management.

The TSO will coordinate:

- the approximate pick up time,
- the name of the individual from the IT Security Office who will physically pick up the equipment, and
- who to contact at the department where the hardware is located.

The IT Security Office employee picking up the equipment will present their SDSU ID card to the department point of contact and fill out the SDSU IT Security Office Equipment Receipt form. Both the IT Security Office employee and manger will sign the form. A copy of the form will be left with the manager and another copy placed in the IT Security Office incident file. Figure P-1 illustrates the equipment receipt used by the IT Security Office for hardware retention.

Once the hardware has been retained, the manager should prepare for resumption of duties without the hardware, as it may not be returned for several weeks or months. The TSO will keep the manager apprised of the hardware status until it is returned, or permanently stored to respond to anticipated legal actions.

Figure O-1: Equipment receipt used by the IT Security Office for hardware retention

SDSU IT SECURITY OFFICE EQUIPMENT RECEIPT FORM

Date:	***Time:***	***Department:***
Equipment Removed:		
Comments:		
ITSO Employee Printed Name:	***ITSO Employee SDSU Card#:***	***ITSO Employee Signature:***
Manager Printed Name:	***Manager Signature:***	***Receipt Number:***

For updated information on this incident please email security@sdsu.edu or call ***(619) 594-0142***

USE THIS RECEIPT NUMBER AS A REFERENCE

For further information and IT Security Office policies, please see http://security.sdsu.edu