

Forensic Responsibility Chart

This chart lists suggested actions involved in carrying out a forensic examination of IT equipment involved in a potential policy violation at NDSU. This chart may be used in conjunction with "NDSU Procedural Guidelines for Investigation of Employee Violations of Acceptable Use of Electronic Communications Devices." The chart shows the responsibility level for each Action for each Actor. Joint action is indicated by more than one "R" indicator for a particular Action.

Participation Key:

A: Approves the plans or selects options for the Action
R: Responsible for carrying out the Action
C: Consulted before the Action is carried out
I: Informed about Action after it is carried out
N: Not involved in the Action

Assumptions:

- (1) Every Action has to be approved by an "authority" above the Actor with Responsibility, at least implicitly.
- (2) Any Action for which an ITS employee is Responsible must be approved by the CIO, to protect the ITS employee.
- (3) In some cases, an Actor may both Approve and be Responsible for an Action.

Last Updated: April 14, 2004

Action Step	Action Category	Action	Actors						Typical Schedule
			AU Review Committee	Provost or Vice Pres.	Dean or Director	CIO	ITS Security Officer	ITS Technician	
FE 1	Prior to examination	Approve initiation of equipment seizure and forensic report process including the initial scope.	C	A	R	C	C	N	When alleged policy violation warrants
FE 2	Prior to examination	Inform Actors about expected forensic examination.	C	N	A/R	N	I	I	As soon as possible
FE 3	Prior to examination	Document the location of the scene.	N	N	A/R	N	I	N	As soon as possible
FE 4	Prior to examination	Secure and evaluate the scene.	N	N	A/R	N	C	N	As soon as possible

Action Step	Action Category	Action	Actors						Typical Schedule
			AU Review Committee	Provost or Vice Pres.	Dean or Director	CIO	ITS Security Officer	ITS Technician	
FE 5	Prior to examination	Conduct preliminary interviews to gain a general understanding of the surroundings, those who work there, the equipment used, need for replacement equipment, etc.	N	N	A/R	N	C	I	As soon as possible
FE 6	During equipment seizure	Remove staff from the scene as appropriate.	N	N	A/R	N	I	N	During equipment seizure
FE 7	During equipment seizure	Document the physical scene, including photographing the scene with a video camera, without moving anything or touching the computer.	N	N	I	A	R	N	During equipment seizure
FE 8	During equipment seizure	Label and inventory all equipment, media, and other evidence to be seized on an ITS "seizure record" form.	N	N	N	A	R	C	During equipment seizure
FE 9	During equipment seizure	Obtain any necessary passwords from the user. Note the passwords on the "seizure record" and have the accused user initial the form.	N	N	A/R	N	C	N	During equipment seizure
FE 10	During equipment seizure	Remove the computer or other equipment and related media from the scene by disconnecting all cables and attached devices, and taking the device to the ITS offices.	I	N	I	A	R	R	During equipment seizure
FE 11	During equipment seizure	Arrange for a substitute computer for the user if appropriate..	N	N	C	A	C	R	During equipment seizure
FE 12	Securing evidence	Store the device(s) and media in a locked area controlled by ITS.	I	N	I	A	R	R	Immediately after equipment seizure
FE 13	Securing evidence	Copy the hard drive to another device or media for examination.	N	N	N	A	R	C	Immediately after equipment seizure
FE 14	Examination	Examine and assess the copy of the contents of the seized hard drive.	C	C	C	A	R	N	Within 1 working day after equipment seizure
FE 15	Examination	Save the evidence on "read only" media; label the media.	N	N	N	A	R	C	Within 1 working day after equipment seizure

Action Step	Action Category	Action	Actors						Typical Schedule
			AU Review Committee	Provost or Vice Pres.	Dean or Director	CIO	ITS Security Officer	ITS Technician	
FE 16	Examination	Evaluate the evidence.	C	N	R	C	C	N	Within 3 working days after equipment seizure
FE 17	Reporting	Prepare a report on the examination of the contents of the hard drive.	C	I	C	A	R	N	Within 3 working days after evidence evaluation
FE 18	Reporting	Approve report	C	A/R	C	N	N	N	Within 3 working days after report is written
FE 19	Reporting	Distribute the report to appropriate Actors.	I	A	R	I	I	N	Within 2 working days after report is approved
FE 20	Retain Evidence	Retain evidence (copy of hard drive, read only media, logs, and reports) as long as required by law. In some cases original devices may need to be retained. In other cases devices may have to be processed (scrubbed, reinstalled, etc.) for return to the original location.	C	N	C	C	R	N/C	As long as required