Idaho Department of Correction	**Standard Operating Procedure**	Title: **Telephones and Electronic Communication Systems: Resident**		Page: 1 of 18
		Control Number: **503.02.01.001**	Version: **9.0**	Adopted: 08/15/1995

Chad Page, chief of the Division of Prisons, approved this document on 11/09/2020.

Open to the public: ☒ **Yes**

SCOPE

This SOP applies to all Idaho Department of Correction (IDOC) facilities to include central office, resident telephone system vendor, contract facilities (where applicable), correctional facilities, and community reentry centers (CRCs).

Revision Summary
Revision date (11/09/2020): Version 9.0: Updated terminology, moved the *Electronic Mail Contraband and Denial Form* to the forms pages for staff convenience, and added verbiage clarifying that providing copies (whether printed or electronic) to residents of any content from the electronic communications system is prohibited.

TABLE OF CONTENTS

BOARD OF CORRECTION IDAPA RULE NUMBER 503

Telephones

POLICY CONTROL NUMBER 503

Use of Telephones by Residents

PURPOSE

The purpose of this standard operating procedure (SOP) is to establish rules and procedures for monitoring and recording resident telephone calls using the IDOC resident call management system (RCMS) and electronic communications system (ECS) to include rules regarding privileged communications between a resident and an attorney.

RESPONSIBILITY

IDOC Leadership

The director of the IDOC, chief of the management services division, and chief of the prisons division or their designees are responsible for implementing this SOP in their respective areas of responsibility.

Chief of the Prisons Division

The chief of the prisons division is responsible to designate a staff member to serve as the prisons intelligence coordinator assigned to the special investigation unit.

Chief of the Management Services

The chief of management services or designee is responsible for:

- Providing oversight of the applicable vendor contracts.
- Identifying a contract administrator.
- Ensuring that the telephone vendor installs telephone-monitoring software that informs the caller and recipient (a) from what facility the call originates, and (b) that the telephone call may be monitored and recorded.
- Ensuring that the ECS vendor uses security filters and provides notices to the public and residents regarding rules and procedures.
- Ensuring all authorized attorney telephone numbers are properly configured as privileged and are not recorded as explained in section 8, Attorney Telephone Calls.

Managers and Facility Heads

Managers and facility heads or designees are responsible for:

- Recommending specific staff members to be granted access to the RCMS and ECS
- Ensuring IDOC employees and contractors are practicing the guidelines, standards, and procedures provided herein

Special Investigations Unit (SIU) Intelligence Coordinator

The SIU intelligence coordinator (hereafter referred to as intelligence coordinator) is responsible for:

- Overseeing the resident telephone and ECS monitoring practices
- Maintaining a list of staff members approved to access the RCMS and ECS.

Contract Administrator

The contract administrator (located in the contract services bureau) is responsible for ensuring the contract providers fulfill all obligations as required in the contract and monitors all operational practices as defined within the scope of work.

STANDARD PROCEDURES

1. Overview of RCMS and ECS

The Idaho Department of Correction (IDOC) requires that the RCMS and ECS have monitoring and recording capabilities for safety, security, and investigatory purposes. For reasons of confidentiality and security, providing copies to residents of ECS communications, whether printed or electronic, is prohibited.

RCMS and ECS use is a privilege, not a right, and nothing in this SOP should be construed to mean that such access or use is a right.

Staff **v**iolating the provisions of this SOP may be subject to corrective or disciplinary action in accordance with SOP 205.07.01.001*, Corrective or Disciplinary Action*.

2. Notification of Monitoring and Recording

Telephones

Residents and members of the public must be informed that telephone calls are recorded and may be monitored.

- The telephone vendor must ensure that the RCMS software informs residents and the public that telephone calls are recorded and may be monitored.
- The contract administrator must ensure that the RCMS vendor provides signage, which states that calls are recorded, may be monitored, and that the signage is posted near RCMS telephones.

Electronic Communication System

Residents and members of the public must be informed that all types of ECS (email, secure photo share, video messaging, etc.) are archived and may be reviewed at any time.

- The communications vendor must ensure that the ECS software informs residents and the public that forms of communications are archived and may be reviewed at any time.
- The contract administrator must ensure that the ECS vendor provides signage or kiosk communication, which states that all ECS mediums are archived and may be reviewed.

3. Telephone Call Rules

Residents must adhere to the following when using the RCMS:

- Follow the rules described in this SOP, facility rules, and SOP 318.02.01.001, *Disciplinary Procedures: Resident*.
- Only place a telephone call to the number dialed
- Must not forward calls to another telephone number
- Must not place three-way calls
- Must not use another resident's personal identification number (PIN) to place a phone call

Any attempted or actual violation of the telephone rules or any attempt to circumvent the RCMS is prohibited and may result in one or more of the following:

- Taking disciplinary action in accordance with SOP 318.02.01.001, *Disciplinary Procedures: Resident*
- Temporarily blocking all telephone numbers involved in the violation
- Restricting telephone call privileges
- Restitution for stolen funds used to pay for calls using another resident's PIN

4. Electronic Communication System

Residents may utilize vendor-provided hardware and purchase ECS devices that support music, email, digital photographs, video messaging, and other services as approved and authorized by IDOC.

Electronic communications via the ECS are not considered privileged or confidential. Electronic communication services (ECS) are provided under contract with an outside third party, and residents must pay to utilize such services. The IDOC does not bear the cost of ECS for on behalf of indigent residents.

Residents may not use the ECS to directly contact IDOC staff.

Electronic communication services automatically transfer with a resident as they move housing units or facilities. Services through the ECS solution are generally available to a resident within three working days of each transfer.

Once released from IDOC custody, communication services through the ECS stop immediately. Residents cannot continue to access the ECS or receive electronic communications via the ECS solution after release.

Prohibited Content

Use of the ECS is subject to the same rules as other means of mailed communication. The following uses and/or content are expressly prohibited:

- Receiving any contraband or anything of an illegal or threatening nature
- Soliciting or accepting any publication or item that has not been paid for in advance
- Obligating oneself or others to time payments
- Joining or participating in book, record, tape, or CD clubs, either personally or via a third party
- Using coercion, threats, or fraud to obtain money, favors, or anything of value
- Sending or receiving email, photo share, or communications for another resident
- Sending or receiving email with coded messages
- Directing or conducting any business operations, except as necessary to protect real property or close out a business
- Soliciting or receiving any information that describes the manufacture of weapons, bombs, explosives, alcohol and drugs, drug paraphernalia, or escape materials
- Role-playing games and related materials
- Sending or receiving information related to the crime, sentence, or identity of another resident
- Sending or receiving publications or items showing gang involvement or activities (enemy lists, constitutions, structures, codes, signs, symbols, photographs, drawings, training material, clothing, etc.)
- Sending or receiving information advocating that any ethnic, racial, or religious group is inferior or that make such groups an object of ridicule and scorn
- Sending or receiving information that encourages violence
- **Sexually explicit, nudity or pornographic material** to include pictorial depictions of nudity, graphic images, personal pictures, drawings, photocopies, or video messages.
    - **Nudity** in this SOP means a pictorial depiction where male or female genitalia, anus, or the nipples or areola of female breasts are exposed.
    - **Sexually explicit** in this SOP means a pictorial depiction of actual or simulated sexual acts including sexual intercourse, oral sex, or masturbation.
    - **Pornographic material** in this SOP includes individual pictures, photographs, or drawings of nudity or sexually explicit conduct to include digital photographs, scanned images, or video messages.
    - Publications, drawings, photocopies, and other pictorial materials that meet the description of nudity in this section, but the person has clothing or other covering that is transparent or virtually transparent.

Note: The following are permitted: Written content of a sexual nature, publications that do not feature nudity, but contain nudity illustrative of medical, educational, or anthropological content may be excluded from this definition.

5. Censored or Discarded Electronic Content

The ECS automatically screens all electronic content for key words and phrases and for any attachments. Any electronic communication which contains key words or phrases or which has an attachment(s) is automatically flagged and held for IDOC staff review before it can be delivered to its intended recipient.

Each facility must have adequate staff assigned to and responsible for reviewing all held electronic communications. When reviewing electronic communication content, reviewing staff must only discard those emails or attachments that violate content rules in this SOP. If an email's content is permitted but an attachment is not, only the prohibited attachment is discarded and the balance of the email and other attachments, if any, are delivered electronically to the resident. However, if the email's content is prohibited but the attachment would otherwise be permitted, limitations of the ECS require that the email and the attachments be discarded.

Each facility's assigned ECS staff has the responsibility to review all flagged electronic communications for content and to ensure that no contraband or prohibited content is allowed to be sent through the ECS.

If contraband or prohibited content is identified, the assigned ECS staff member making the determination must follow the process set forth below, including completion of the *Electronic Mail Contraband and Denial Form* and delivering the form to the resident. In addition to the staff completing a hard copy of the *Electronic Mail Contraband and Denial Form*, the ECS automatically notifies the resident when electronic content has been discarded. The resident is not refunded for discarded content.

Members of the public receive only the electronic notice that content was discarded and the public is not refunded for discarded content. Any electronic communication that is censored or discarded due to content remains stored on the ECS. After six months, content and emails may be archived by the ECS but are still accessible to IDOC staff by contacting the ECS provider.

Contraband--Electronic Communications

Functional Roles and Responsibilities	Step	Tasks
Assigned Staff	1	Within five business days, access the ECS to review all held or flagged electronic communications.
	2	View each digital photo or greeting card and watch each VideoGram to determine if any of the content is prohibited.

Functional Roles and Responsibilities	Step	Tasks
Assigned Staff	3	Take the following actions based on the type of contraband found in an electronic communication: • Approved content – release the electronic communication for delivery to its intended recipient (process ends here). • Prohibited content (no attachments) – select from the available categories that indicate what or why the content is prohibited and discard the entire email. Complete the *Electronic Mail Contraband and Denial Form* and provide to resident. • Prohibited content in attachments – (a) select the attachment(s) that contains the prohibited content and mark as "discard", (b) select from the available categories what or why the content is prohibited (c) discard the prohibited content and release the remaining electronic content (and attachments if any) for delivery to its intended recipient. Complete the *Electronic Mail Contraband and Denial Form* and provide to resident. (Process ends here). • Prohibited email (with attachments) - select from the available categories what or why the entire content is prohibited and discard the entire email and all attachments. Complete the *Electronic Contraband and Denial Form* and provide to resident. • Emails containing perceived security or safety risks or which are determined to need further review are to be flagged "sent to security" and the ECS automatically holds for further review by investigations staff. • Anytime an electronic communication or any attachment is discarded due to prohibited content, the staff member who took such action must print *Electronic Mail Contraband and Denial Form*, complete it as required, and provide a copy to the resident.

Functional Roles and Responsibilities	Step	Tasks
Investigations Staff	4	Within five business days, review electronic communication flagged “sent to security”. • Approved content – release the electronic communication for delivery to its intended recipient. • Prohibited content (no attachments) – select from the available categories that indicate what or why the content is prohibited and discard the entire email. • Prohibited content in attachments – (a) select the attachment(s) that contains the prohibited content and mark as “discard”, (b) select from the available categories what or why the content is prohibited, and (c) discard the prohibited content and release the remaining electronic content (and attachments if any) for delivery to its intended recipient. Complete the *Electronic Mail Contraband and Denial Form* and provide to resident. (Process ends here). • Prohibited email (with attachments) - select from the available categories what or why the entire content is prohibited and discard the entire email and all attachments. • Anytime an electronic communication or attachment is discarded due to prohibited content, the staff member who took such action must print *Electronic Mail Contraband and Denial Form*, complete it as required, and provide a copy to the resident.

6. Suspending RCMS and ECS Access

Facility heads or designees can temporarily suspend a resident’s RCMS or ECS access or block specific telephone numbers, or email addresses or resident access for investigative purposes. Disciplinary hearing officers (DHOs) can suspend a resident’s RCMS or ECS privileges as a disciplinary sanction in accordance with SOP 318.02.01.001, *Disciplinary Procedures: Resident*. Any member of the public can request a block on their phone number without a hearing or administrative action. Any member of the public can discontinue email by cancelling their account.

To suspend a resident’s RCMS or ECS access beyond the investigation or disciplinary sanction, the IDOC conducts an administrative hearing (the access restriction can be to one or more methods of ECS or RCMS depending on the security risk or rule violation). The administrative hearing is similar in structure to a resident disciplinary hearing. The hearing is recorded, the hearing officer must advise the resident of the allegations and the

department's intention to initiate long-term restriction of RCMS or ECS or both and allow the resident to show cause why long-term restrictions should not be imposed. To initiate this process the facility head or manager must contact the prisons division disciplinary coordinator and the applicable deputy chief or CRC operations manager. The prisons division disciplinary coordinator assists the facility with the hearing process and selection of the hearing officer. A disciplinary hearing officer or similarly trained staff must conduct the hearing and provide the prisons division chief with an audio recording of the hearing.

The prisons division chief or designee makes the final decision regarding long-term restrictions in consultation with the facility head or manager.

Restrictions on ECS access would not generally include restrictions on commissary access so if long term ECS restriction is approved, facility staff will provide the impacted resident with an alternative means of ordering commissary, acceptable to the contracted commissary provider.

7. Purchase of Telephone Time and Refunds

For telephone time purchase and refund information, see SOP 114.04.02.001, *Funds: Resident*. For the purchase of ECS device and related products, see SOP 406.02.01.001, *Commissary.*

8. Attorney Telephone Calls

Telephone calls between a resident **a**nd an attorney, placed to the attorney's business telephone number as listed with the Idaho State Bar, are not monitored or recorded. Voice messages left by an attorney using the resident phone system for an resident are not privileged, are recorded, and can be monitored.

The contract administrator or RCMS vendor must obtain, from the Idaho Bar, the business telephone numbers of all Idaho attorneys and provide the numbers to the RCMS vendor. The RCMS vendor must program the RCMS so that calls made to Idaho attorney telephone numbers cannot be monitored or recorded.

Attorneys may request to have their business telephone number added to the non-monitored list. Requests must be sent to the contract administrator on the attorney's official letterhead. The contract administrator must use the appropriate state bar website to confirm the attorney is active and in good standing with the bar, and verify the name, address, and telephone number of the attorney. If the telephone number is verified, the contract administrator provides the name and contact information to the SIU chief investigator or designee and the prison division's chief for review prior to adding it to the RCMS. Once approved by the SIU chief investigator and prison division's chief, the contract administrator adds the number and notifies the attorney in writing when the programming is complete.

An attorney can request to add a secondary number to the non-monitored list. The request must be made using the attorney's letterhead, signed by the attorney representing the resident, and sent to the contract administrator**.** Proof of ownership by means of a billing statement for the number must be provided. Personal information can be redacted from the billing statement, but name, date, account number, and telephone number must be visible. If the number is a second office and the contract administrator can independently verify that is the attorney's place of business, the billing statement is not required. The contract

administrator forwards the request to the SIU chief investigator and the division of prisons chief. The division of prisons chief approves or denies the request and notifies the contract administrator who must take appropriate action, notifying the requesting attorney in writing of the decision and actions taken.

Charges for Attorney Calls:

Calls to a resident's attorney cost the same as calls to members of the public. The resident can pay for the call using their own funds or, if the attorney has set up a prepaid account with the RCMS provider, use said prepaid funds. Exception: Resident's calls made to their public defender of record are free of charge if the public defender has contacted the contract administrator and provided the required documentation.

Attorney Agent Calls

Note: Except for exceptional circumstances, telephone numbers of attorney agents are not added to the non-monitored list.

The request and approval processes are the same as the process for adding a second number. If the request is approved, a specific length of time must be established. If the attorney needs additional time, he must submit another request. The division of prisons chief approves or denies the request and notifies the RCMS contract administrator who must take appropriate action, notifying the requesting attorney in writing of the decision and actions taken.

If the RCMS vendor receives any requests to add numbers to the non-monitored list, the RCMS vendor must forward the requests to the contract administrator. The contract administrator must use the applicable process established in this section.

Non-Monitored List Management

The contract administrator audits the non-monitored list monthly to ensure that numbers have been approved in accordance with this section. The non-monitored list is forwarded to the SIU investigation chief and division of prisons chief monthly.

Unintended Recording of a Resident/Attorney Telephone Call

If a resident-attorney telephone call (to the attorney's business number) is inadvertently recorded, the staff member must not listen to the call or immediately stop listening when the staff learns that the call is to an attorney and must not share any of the conversation with other staff, except as noted in the next subsection. The staff member must immediately notify his manager or facility head or designees. The manager or facility head or designees must verify that it is an attorney's authorized business number and if verified, ensure the number is programmed as a non-monitored number in the RCMS. Once verified that it was an attorney business number, any recorded call to that number must be deleted from the RCMS.

If the attorney telephone call was to a number that was not an authorized business number, the facility head or designee must notify the attorney of the following:

- That the telephone number is not on the non-monitored list
- That the attorney's business number recorded with the Idaho Bar is on the non-monitored list

- The process if the attorney wants to request adding an additional number to the non-monitored list

Suspected Misuse of Resident/Attorney Telephone Call Privileges

If a staff member has reason to believe that a conversation or call violates IDOC or facility rules, jeopardizes the facility's secure and orderly operation, or that a crime has been or may be committed, the staff member must immediately report it to his manager or facility head or designee. The staff member must describe how the information was obtained. The manager or facility head or designees must discuss the issue with the prisons division chief or designee (see SOP 604.02.01.002, *Attorney and Professional Staff Access to Residents,* for further information).

The prisons division chief or designee may take action, to include, but not limited to, one or more of the following:

- Advising the attorney that violating IDOC or facility rules may result in his telephone number being blocked from receiving calls from the RCMS
- Terminating telephone calls between the resident and the attorney by having the telephone number(s) blocked
- Reporting the matter to the appropriate authorities, including law enforcement

Electronic Communication System

Attorney communications using email, digital photograph, and video messaging are not privileged, are archived and may be reviewed.

9. Levels of Staff Access

The RCMS and ECS have the following levels of access:

System Administrator

Full system access with the ability to perform all functions, services and applications associated with the RCMS or ECS system at all other levels. System administrator access is limited to the contract administrator, the intelligence coordinator, and others as specifically approved by the prison division chief or deputy chief or designee.

Site Administrative

Site Administrative access includes monitoring and investigator level 1 access plus the ability to reset personal identification numbers (PIN) and personal access numbers (PAN), reset name recording, and restrict RCMS and ECS access.

Access to PIN-PAN is for basic functions such as managing PINs, restricting PAN, and restricting calls to a personal telephone number at the owner's request.

Monitoring

Monitoring includes PIN-PAN, PREA, telephone call monitoring, and ECS monitoring. In addition, can monitor recordings at all sites, monitor live calls, forward live calls, review calls from all sites, view notes made on individual calls.

Monitoring is for staff members who listen to RCMS conversations and review ECS email, digital photographs, video messages, etc. for official IDOC business, but do not need system management functions.

Investigators

Investigator level 2 includes PIN-PAN, monitoring, PREA, and monitoring, can listen to restricted calls (numbers marked restricted such as the facility informant line or other specialty numbers with tightly controlled access) create compact disk (CD) queues, and burn calls and ECS information to a CD, or other storage device.

Investigator level 2 includes the ability to save telephone conversations as audio files. To ensure security of recorded conversations, this position is limited to two individuals per facility. The prisons division chief is the approval authority to any exception to the two-person limit.

Prison Rape Elimination Act (PREA) Tip Line

This access is limited to monitoring PREA tip lines. Access is typically facility administrative staff and on duty staff members such as shift commanders and assistant shift commanders who can respond to potential victims of sexual assault.

Outside Law Enforcement

This access is limited to reviewing archived calls placed by IDOC residents, download calls and access to investigative or mapping tools. To ensure security of recorded conversations, the prisons division chief or designee approves law enforcement access.

10. Approving Staff Access to RCMS and ECS

Access to the RCMS and ECS is limited to individuals with a legitimate need such as assigned staff, investigators, second in command, facility heads, and individuals with administrative duties required to operate the system.

The chief of the prisons division may grant law enforcement agencies access to the RCMS and ECS. To limit the number of people aware of such access, the prisons division chief works directly with the intelligence coordinator when authorizing and implementing access. When access is authorized, the intelligence coordinator either adds the authorized access or contacts the contract administrator for implementing access. The intelligence coordinator must provide the approved agencies with a *Non-Disclosure Release Form.* The IDOC may revoke access if an agency violates the non-disclosure guidelines.

To change staff access during the year, the facility head notifies the intelligence coordinator via email. In consultation with the chief of the prisons division, the intelligence coordinator updates the authorized list and notifies the contract administrator to implement access.

The intelligence coordinator can have a staff member’s access removed when needed.

This process is used to establish access to RCMS and ECS initially and then used annually for reauthorization. Access rights expire annually and reauthorization must be obtained each year. Requests for initial authorization and reauthorization must be made using the following steps:

Functional Roles and Responsibilities	Step	Tasks
Facility Heads or Designees	**1**	• By December 1 each year, complete *RCMS and ECS Access Request.* • Include up to two investigator level-2 staff. • Submit the completed information to the intelligence coordinator.
Intelligence Coordinator	**2**	• Ensure that each facility has submitted an *RCMS and ECS Access Request*. • Complete an Electronic Communication Access Request for any additional staff who requires access. • Review each *RCMS and ECS Access Request* and document any concerns. • By December 15, forward the *RCMS and ECS Access Requests* to the applicable prisons division deputy chiefs and the CRC operations manager.
DOP Deputy Chiefs and CRC Operations Manager	**3**	• Review each applicable facility *RCMS and ECS Access Request* • Resolve any concerns with the applicable facility head. • Complete the *RCMS and ECS Access Request*. • Forward the completed *RCMS and ECS Access Request* to the intelligence coordinator.
Intelligence Coordinator	**4**	• Develop a list of the authorized individuals including the level of access authorized. • Forward the information to the contract administrator. • Notify facility heads of those authorized to access the electronic communication at their respective facilities. • File the signed request forms (maintain for two years and then dispose of the forms).
Contract Administrator	**5**	Ensure that the vendor provides access to the authorized individuals.

11. RCMS and ECS Security

To reduce risk of unauthorized access to the RCMS or ECS, monitoring staff members must only use computers in secured locations that residents cannot access and cannot use multi-user computers such as a control center, officer station, etc.

Staff members authorized must not allow anyone access to RCMS or ECS or give their system login or password information to anyone.

When a staff member no longer requires access to the RCMS or ECS or both, the intelligence coordinator or contract administrator removes the staff member from the approved list and ensures that access to the applicable system is removed.

12. Information Security

Only staff members authorized as described in section 10, can access and monitor RCMS and ECS. Intercepted information that does not pose a risk must not be shared or discussed among staff members. Intercepted information that poses a risk to the safety or security of the facility, safety of staff, public, or residents, or is criminal in nature is only discussed or shared with staff members who are authorized to receive such information and have a need to know.

With exception of the intelligence coordinator, contract monitor, and SIU investigators, staff members must only monitor the restricted numbers (“tip line”) at the facility to which the staff member is assigned (see SOP 504.02.01.001, *Investigations and Intelligence Program* for further information regarding “tip lines”).

Public Access

Recorded conversations, data reports, call logs, emails, digital photographs, video communications etc., are not open to public disclosure and can only be released to the individuals and agencies listed below. The prisons division chief or designee can authorize individuals on a case-by-case basis to have access to the RCMS or ECS or to receive messages or information recorded on the systems.

The following are authorized to receive RCMS and ECS files:

- IDOC director
- Deputy attorneys generals assigned to IDOC
- SIU investigators
- Prisons division chief
- Prisons division deputy chiefs
- CRC operations manager
- District managers (only when directly related to probation or parole violations)
- Department disciplinary oversight coordinator(s) (only directly related to DORs)
- Facility disciplinary hearing officers (limited to evidence presented at a DOR hearing)
- Facility heads
- Deputy wardens (second in command and DOR review and appellate authorities)
- Serious incident review (SIR) committee
- Staff authorized in accordance with section 8
- Law enforcement agencies (for criminal investigation purposes)

13. Release of RCMS and ECS Files

RCMS and ECS used in IDOC administrative investigations, administrative hearings, or criminal investigations that are provided to others are managed using the following steps. (**Caution:** Anyone releasing information to an outside law enforcement agency, court, or any other entity must follow the steps described in this section.)

Functional Roles and Responsibilities	Step	Tasks
Requesting Staff or Agency	**1**	Submit a request to a facility investigator, SIU investigator, or intelligence coordinator for recorded conversation or ECS medium. State the purpose of the request, such as administrative investigation or review, DOR evidence or review, criminal investigation.
Facility Investigators or SIU Investigators	**2**	Request a log number from the intelligence coordinator.
SIU Intelligence Coordinator	**3**	• Ensure the request meets the requirements of this SOP. • Request additional information if necessary.
	4	Request does not meet the requirements of this SOP: • Deny the request and notify the facility investigator or SIU Investigator. • Do not download, save, or release the information. • Notify the requesting party that the information cannot be released in accordance with IDOC policy. (The process ends here.) Request meets the requirement of this SOP: • Issue a log number and document the request. • Notify the authorized staff.
Authorized Staff	**5**	• Identify the RCMS or ECS file. • Save the file(s) in an applicable format. • Forward the file(s) to the requesting party. • If the individual is not an authorized IDOC staff, also forward a completed copy of *Non-Disclosure Release Form.*
Requesting Party	**6**	• Destroy copies of files used for IDOC administrative hearings and other administrative functions after the hearing or issue is resolved. • Store copies of files used for IDOC investigations in accordance with section 14.

		• Copies of files sent to law enforcement agencies are retained in accordance with each agency's policy.

14. Interception of Suspicious Telephone Calls or Email Activity

If while monitoring RCMS or ECS, a staff member learns of information that indicates criminal activity, violation of department or facility rules, is a risk to facility safety or security, or indicates staff misconduct, he must immediately notify the applicable authority in accordance with this section. If a contract provider or contract administrator learns of information related to criminal activity or that threatens the safety or security of a facility, or safety of the public or staff, he must immediately contact the intelligence coordinator.

Staff at contract facilities and other contract staff must report information related to residents under IDOC jurisdiction, IDOC facilities, and staff to both the manager or facility head and the contract prison oversight unit deputy warden or designee.

Criminal Activity Not Involving Residents under IDOC Jurisdiction

IDOC investigators learning of information about criminal activity that does not involve residents under the jurisdiction of the department must immediately notify the law enforcement agency with jurisdiction. Requests for copies of the relative information must be in accordance with section 12, Release of RCMS or ECS Files.

Activity Involving Residents under IDOC Jurisdiction or IDOC Facilities

IDOC investigators must report to the facility head or appropriate manager information regarding:

- Criminal activity.
- Activity presenting a risk or potential risk to the security or safety of an IDOC facility.
- Activity presenting risk to the safety of staff, public, or residents.
- Information regarding behavior or activities that violate IDOC facility rules.

The applicable manager or facility head takes one or more of the following actions:

- Immediately place a temporary block the resident's use of the RCMS or the resident's ability to call certain numbers, restrict use of the kiosk, or specific functions of the kiosk.
- Initiate disciplinary action.
- Request further telephone and ECS monitoring and investigation.
- Refer to special investigations unit.
- Authorize release of the intercepted information to an outside law enforcement agency or court.

Staff Misconduct

Any information indicating possible staff misconduct must be reported immediately to the applicable manager or facility head.

15. RCMS and ECS Recording Retention

RCMS recordings must be maintained in the system for three years or longer.

ECS video recordings are actively maintained for 60 days.

Emails are maintained for three years or longer.

Digital photographs are maintained for three years or longer.

Copies of recordings used in IDOC investigations become part of an investigative file and maintained in accordance with SOP 116.01.01.001, *Custody of Evidence: Special Investigations Unit* and SOP 504.02.0.001, *Investigations and Intelligence Program.*

16. Requests for Blocking and Unblocking Access

Telephone numbers can be blocked as follows:

- All IDOC facilities
- Specific IDOC facilities or
- Specific residents

The Public

Members of the public may have their personal telephone numbers blocked or unblocked from receiving telephone calls by selecting the correct prompt through the RCMS, contacting the RCMS provider, contacting the facility, or the contract administrator. Requested blocks remain in place for a minimum of 30 days if the requesting person asks to have the number unblocked. If the department suspects or experiences abuse of the blocking or unblocking process, written requests may be required.

Members of the public may have their personal email address blocked by canceling their ECS access account.

Staff Members

Staff members must not accept unauthorized telephone calls from the RCMS or initiate ECS. If a staff member inadvertently accepts an unauthorized call from a resident, he must report it the next working day to the facility head, manager, or designee.

To obtain authorization to receive telephone calls or set up ECS with a specific resident such as a family member, staff members must report the relationship in accordance with Policy 218, *Non-Fraternization with Residents,* and request authorization.

Any staff member can submit a request to the facility head or designee to have his personal telephone number blocked from the RCMS calls.

DEFINITIONS

Attorney Agent: A person, qualified through education, training, or work experience performing specifically delegated legal work, employed or retained and directly supervised by an active attorney member of the Idaho State Bar, another state's bar, or a government agency. The supervising attorney must maintain a direct relationship with the resident client represented.

Attorney Telephone Call: A verifiable, unmonitored, and unrecorded telephone call between an resident and an attorney

Public: A person (of the public) that does not include residents, contractors, vendors, volunteers, interns, or the employees of the Idaho Board of Correction, Idaho Department of Correction (IDOC), or Commission of Pardons and Parole.

Three-Way Call: A telephone call that adds a third person to a telephone conversation between two people via a single phone line, thereby allowing all three people to hear and speak to each other via that single call

REFERENCES

Electronic Mail Contraband and Denial Form

RCMS and ECS Access Request Form

Non-Disclosure Release Form

114.04.02.001, *Funds: Resident*

116.01.01.001, *Custody of Evidence: Special Investigations Unit*

205.07.01.001, *Corrective or Disciplinary Action*

218, *Non-Fraternization with Residents*

318.02.01.001, *Disciplinary Procedures: Resident*

406.02.01.001, *Commissary*

504.02.0.001, *Investigations and Intelligence Program*

604.02.01.002, *Attorney and Professional Individual Access to Residents*

– End of Document –