CIDDD Exhibit P-0024 Page 1

Royal Newfoundland Constabulary

Policy and Procedure Manual
General Order 322
December 10, 2013

Information Management and Technology

1.0 General

1.1 The purpose of this policy is to establish the framework within the Royal Newfoundland Constabulary achieve the greatest benefits from the use of information and technology.

a. It will Identify data bases and information systems in use and provide users with guidelines and direction regarding the operation of same.

1.2 Information management and technology are core components of the RNC's infrastructure.

1.3 The Information Services Division is responsible for planning, developing, organizing, directing and managing the Information Management and Technology program in partnership with the Office of Chief Information Officer (OCIO).

2.0 Office of Chief Information Officer (OCIO)

2.1 The OCIO is the central authority for the Government of Newfoundland and Labrador, and provides Information Technology and Information Management services to the RNC.

2.2 The services provided are governed through a **Service Level Agreement** which defines the scope, level and quality of Information Technology and Information Management services the OCIO provides the RNC. This agreement describes roles and responsibilities, mechanisms for communication, the dispute resolution process, and the process for adding new services.

2.3 There are a variety of policy, guidelines, standards, directives and memoranda that support policy located on the OCIO Website.

3.0 Information and Technology Security

3.1 Security is the responsibility of all employees that have access to, use or manage the information and technology assets of the RNC. Information systems security includes the protection of personal data, systems, documentation, computer-

CIDDD Exhibit P-0024 Page 2

generated information and facilities, from accidental or deliberate threats to confidentiality, integrity or availability.

3.2 As the initial contact for all employees in the RNC and the OCIO, the Human Resources (HR) Division is responsible for ensuring and achieving the appropriate security clearance for each employee, as required for their job functions.

3.3 All personnel must complete a **RNC Security Clearance**.

3.4 An employee requiring access to CPIC for maintenance or inquiry shall be fingerprinted by the Forensic Identification section and fingerprints submitted to Canadian Criminal Real Time Identification Services (CCRTIS).

3.5 The following information shall be conveyed to the employee.

a. Expectations of Privacy:

(1) Computer equipment and resources are provided to employees to conduct government business. Employees should have no reasonable expectation of privacy as equipment and resources may be monitored, where necessary, by the employer.

(2) Technology exists on the RNC network to monitor systems for security and performance reasons. This technology is capable of monitoring internet and other activity on the network.

(3) OCIO staff has full access to data stored on network drives as it is the OCIO mandate to protect sensitive information as well as its computer and network resources.

b. Electronic Mail:

(1) Employees should be aware that electronic mail remains stored on departmental file servers or backup for 30 days, even after the originator or recipient has deleted the message.

(2) Once electronic mail is sent outside the government's firewalls, it is not secure from interception or alternation unless encrypted.

CIDDD Exhibit P-0024 Page 3

(3) Employees must only use the electronic mail account provided by OCIO/RNC from the network when exchanging email with outside systems.

(4) The RNC/OCIO will perform a periodic review of employees' capacity of email storage.

3.6 The Corporate Services Division (Department of Finance) shall distribute to the OCIO, a monthly report from the payroll system outlining the status changes of employees. This list shall include employees terminated, hired or on leave of absences from their job. This information will be used to modify the employee's access privileges to network resources.

3.7 The Office of Chief of Police or Director of Information Services may at any time notify the OCIO to deny staff access privileges to any network resource.

3.8 Access to the RNC datacenter and data closets in RNC buildings are restricted to RNC/OCIO personnel and authorized employees. Room access log files shall be maintained and the access codes shall be changed annually.

4.0 Appropriate Use of Information Resources

4.1 All users of the RNC's information and technology resources must take responsibility for, and accept the duty to actively protect information and technology assets. This includes taking responsibility to be aware of, and adhere to, all relevant legislation, policies and standards.

4.2 Access to RNC's information and technology resources is for the purpose of conducting RNC business.

4.3. Access by employees to RNC information for personal reasons or non-law enforcement related reasons is prohibited and any improper access by an employee will cause an employee to be subject to discipline up to and including dismissal.

a. Information is only accessible to officers and RNC civilian employees for the purposes law enforcement and related programs and activities.

b. Random audits of officers and civilian RNC employees' access to RNC information will be conducted to ensure there has been no improper

CIDDD Exhibit P-0024 Page 4

access to RNC information for personal or non-law enforcement related reasons by officers or civilian RNC employees.

4.4 Users must use information and technology resources in accordance with applicable terms and conditions.

4.5 Users are required to:

a. ensure reasonable measures are taken for controlling the use of their passwords (passwords should be changed at a maximum of every 90 days) user identification, network and database accounts;

b. use strong identification and authentication to perform two factor authentication for CPIC. PIP, and Outlook Web if a token has been provided;

c. safeguard confidential information;

d. follow the instructions set down by the RNC to ensure network and information security;

e. take reasonable measures to ensure computer viruses are not transferred;

f. notify the OCIO of any viruses encountered immediately;

g. utilize e-mail communication in a professional and business manner (avoid objectionable language); and

h. avoid unacceptable activities that violate accepted departmental and Treasury Board standards (e.g., circulating e-mail containing abusive or sexist messages, pornography, chain letters, jokes, etc.)

4.6 The following conditions are unacceptable and will result in discipline up to and including dismissal.

a. Users must not:

(1) download, view, access or distribute pornographic and/or obscene material;

CIDDD Exhibit P-0024 Page 5

(2) use the Employer's equipment and resources in any way that may be perceived as harassment under the Harassment and Discrimination Free Workplace Policy;

(3) use the Employer's equipment for personal purposes;

(4) participate in activities in violation of federal or provincial laws;

(5) install any hardware including but not limited to; personal USB drives, personal cell phones, personal external hard drives or any peripherals, or software (computer games, screen savers or utilities and any software downloaded from the internet or from another medium) on computers operational within the RNC unless specifically authorized by the OCIO;

(6) access personal email accounts or chat utilities from within the RNC network (Including resources as Hotmail, Yahoo, Facebook, SKYPE, Twitter, or any other social networking message system, etc.);

(7) access radio stations or video clips (typically referred to as "streaming" audio or video) over the internet, unless the access is authorized on a designated workstation with an independent DSL line, is work-related, and authorized;

(8) utilize someone else's user identification or password to gain access to a network resource without proper approval;

(9) read someone's else's electronic mail or employee's information which resides on RNC/OCIO managed resources (e.g. P:\ drive) without proper approval;

(10) send applications, games, movies, music files to other users via e-mail;

(11) configure a government email account to automatically forward incoming messages to a non-government email account;

CIDDD Exhibit P-0024 Page 6

(12) circulate e-mail to large audiences unless it is business related without proper approval (especially RNC or Government wide distribution);

(13) send e-mail attachments larger than 50MB;

(14) circulate virus warnings (only OCIO staff or their designate are permitted to do this);

(15) access the RNC network using their own personal equipment (e.g. personal Laptop, IPad, etc.); and

(16) use of “personal” email tags (inspirational quotes or otherwise) attached to your business signature.

5.0 Information Protection

5.1 Any information obtained in the course of an affiliation with the RNC may be deemed restricted if it meets one or more of the following criteria:

a. any file whereby any sworn or civilian member of the RNC is the complainant, focus or a person of interest in an investigation;

b. any file whereby any immediate family member of any sworn or civilian member of the RNC is the focus or a person of interest in an investigation;

c. any file which may cause discomfort or embarrassment to any employee of the RNC, or which may impede the working environment of the organization; and or

d. any file which requires discretion and/or covertness in order to avoid impeding an investigation.

6.0 Personal Information Protection

6.1 Personal information means recorded information about an identifiable individual, including:

a. the individual's name, address or telephone number;

CIDDD Exhibit P-0024 Page 7

b. the individual's race, national or ethnic origin, color, or religious or political;

c. beliefs or associations;

d. the individual's age, sex, sexual orientation, marital status or family status;

e. an identifying number, symbol or other particular assigned to the individual;

f. the individual's fingerprints, blood type or inheritable characteristics;

g. information about the individual's health care status or history, including a physical or mental disability;

h. information about the individual's educational, financial, criminal or employment;

i. status or history;

j. the opinions of a person about the individual; and

k. the individual's personal views or opinions.

6.2 For further information regarding information protection employees shall refer to OCIO Information Management and Protection policy.

7.0 Roles and Responsibilities

7.1 The Director of Information Services is responsible for promoting and authorizing the effective utilization of technology and information in support of achieving organizational objectives by making informed decisions and recommendations concerning technology applications and information management practices within the RNC.

7.2 OCIO/RNC Support Services is to provide Service Desk, troubleshooting function for software applications and hardware to ensure continuity of service to the end user. Maintaining ongoing operation of desktop and network resources is the core component of this function.

CIDDD Exhibit P-0024 Page 8

7.3 Managers and Supervisors are responsible to monitor the computer function and usage in their areas and report any problems to the Service Desk for follow-up and repair.

7.4 Managers/Supervisors are responsible for:

a. ensuring requests for network and database access are forwarded to the OCIO Service Desk following transfers to any new Division;

b. ensuring that authorized individuals in the Division use their access to departmental systems for government business and other authorized purposes only;

c. ensuring that divisional employees adhere to all network and computer resource usage related policies;

d. investigating any reports of unacceptable computer resources usage by authorized individuals and taking any required follow-up action; and

e. ensuring that employees are aware of the interpretation of “unacceptable use” of departmental network resources.

7.5 To facilitate an employee supervisory duty, Commissioned Officers and Managers in consultation with the Legal Service Unit, may request in writing, for the OCIO to:

a. provide access to a subordinate employee’s e-mail or desktop computer;

b. monitor internet usage of a specific person or computer; and

c. provide access to any subordinate employee’s folder/sub-folders that reside on any RNC/OCIO managed resource(s).

7.6 The Planning and Service Delivery Committee (PSDC) is an appointed committee of employees of the OCIO and RNC. Members of the committee have the authority to act on behalf of their respective parties. The mandate of this committee is outlined in the **Service Level Agreement** between both the RNC and the OCIO.

CIDDD Exhibit P-0024 Page 9

7.7 The RNC PSDC Committee members are the Director of Information Services and Manager of Information Services. These committee members have the authority to manage the RNC discretionary funding allocated from the OCIO.

8.0 *Access to Information and Protection of Privacy Act* (ATTPA)

8.1 This legislation is designed to create a culture of openness and accountability in the public sector while protecting the personal information of citizens and commercially sensitive information of businesses. Its purpose is to:

a. provide the public with the right of access to records; and

b. protect the privacy of individuals whose personal information is collected, used and disclosed by public bodies.

9.0 Disclosing or Sharing of Information

9.1 The *Access to Information and Protection of Privacy Act* requires that:

a. government departments and public bodies must be authorized to collect and use personal and confidential information;

b. access to personal and confidential information is limited to those that need to use it to do their job; and

c. when disclosing information, the minimum amount disclosed to provide a service or complete a transaction.

9.2 Employees shall also refer to the OCIO's Using and Sharing Information - Best Practices.

10.0 Information Systems/Applications

10.1 Police Information Portal (PIP):

a RCMP N-III Police Information Portal (PIP) is a searchable index of all police agency Record Management Systems (RMS) across the country.

b. Detailed PIP policy may be obtained from Information Services Division or can be reviewed on the RNC Intranet.

10.2 Canadian Police Information Centre (CPIC):

a RCMP Canadian Police Information Centre (CPIC) is responsible for the delivery and sharing of national police, law enforcement, criminal justice, and public safety information.

b. The Canadian Police Information Center (CPIC) is a 24- hour "on-line" computer service, giving access to information of police interest concerning persons, property and vehicles across Canada.

c. No unauthorized person shall use or attempt to access CPIC, and the access to CPIC shall be confined to police matters only. Information accessible through CPIC is only for official duties related to law enforcement and related operating programs and activities. Access to CPIC is prohibited for personnel use.

d. Any information obtained through CPIC, police officers must verify the accuracy on that information with the originating agency prior to the use or reliance of the information.

e. Detailed CPIC operating policy which may be obtained from Information Services Division or can be reviewed on the CPIC Web application.

(1) Refer also to Criminal Reporting Procedures policy.

f. CPIC training is made available through Canadian Police Knowledge Network (CPKN).

10.3 Motor Registration Division (MRD):

a. The MRD database application is used to query for license and other driver/vehicle information.

b. Request for access to the MRD system must be forwarded to Information Services Division, attention RMS administrator.

c. The MRD application is installed on a number of computers throughout the organization.

CIDDD Exhibit P-0024 Page 11

d. The MRD Web application is installed on several blackberries, data is unloaded every 24 hours, and officers must verify the accuracy of the information with the Communications Center before proceeding with any action.

e. Front line personnel have access to the license and registration information on MRD to assist with identification of drivers and vehicles. This information is used for police purposes only and shall not be shared with other agencies. Data from these database searches may become part of the police file.

f. The Photo Licensing System (PLS) is an additional module on the MRD system.

(1) Access to the PLS is permitted to be installed only on the computers in the Intelligence and Organized Crime Unit and access to this database is restricted to police officers who work in the Intelligence and Organized Crime Unit.

(2) Access to PLS must be forwarded from the Intelligence and Organized Crime Unit to the System Manager at MRD directly. When a police officer receives access to the PLS they are provided with a copy of the policy which governs dissemination of the data.

(3) When a police officer is transferred out of the Intelligence and Organized Crime Unit a request to remove their access to the PLS must be forwarded from the Intelligence and Organized Crime Unit Supervisor to the Systems Manager at the MRD for action.

(4) All requests for a picture from the PLS will be made using the **Request for Services Form #215**. If the request is approved the photo will be given to the requesting police officer and shall be noted on the form. When the police officer no longer requires the photo it must be returned.

(5) PLS Information (images) shall not to be:

(a) placed in any operational files;

(b) used for evidentiary purposes;

CIDDD Exhibit P-0024 Page 12

(c) distributed to outside agencies;

(d) used in lineups; and/or

(e) used for court purposes

(6) Any problems or issues identified with the PLS should be forwarded to the NCO i/c Intelligence and Organized Crime Unit who will contact the Systems Manager at MRD.

10.4 Integrated Constabulary Automated Network (ICAN):

a. The automated reporting/recording system in use for the RNC is ICAN.

b. The operational and administrative managing authority is the RNC Information Services Division (ISD).

c. All sworn employees of the RNC will be permitted access to ICAN. The extent of privileges will vary from employee to employee. An employee's privileges will be determined by the employee's supervisor in consultation with the ISD.

d. All personnel will receive ICAN training to support the level of privileges that their position requires within the organization. All training will be coordinated through the RNC Training Section.

e. The ICAN system allows for the creation and maintenance of private (restricted) records.

f. The major components of ICAN are:

(1) Computer Aided Dispatch (CAD):

(a) CAD refers to the IT infrastructure used to initiate calls for police assistance, dispatch police resources, and maintain the status of responding resources.

(b) The CAD system:

(i) collects the initial information for an incident and then provides the information to the RMS system;

(ii) assigns a case file number and captures pertinent information used to dispatch to the appropriate units in the field for a response purposes;

(iii) continually monitors, updates, and records unit status, this information may be made available by voice communication or through the mobile data computers;

(iv) maintains the elapsed time between status changes/checks and alerts the dispatcher when thresholds times (dispatched, at scene, cleared) are met;

(v) ensures appropriate access to information and system security (including Table maintenance; security and data management; address maintenance; logging and customization); and

(vi) includes standard reports that can be run using flexible parameters.

g. Records Management System (RMS):

(1) The RNC must maintain records of information relevant to law enforcement activities and public safety in their community (e.g. information related to violation tickets; charges; arrests; evidence; ongoing investigations; and property).

(a) The ICAN Records Management System (RMS):

(i) provides a means by which this information can be efficiently and systematically retained;

(ii) ensures appropriate access to information and system security (including Table maintenance;

CIDDD Exhibit P-0024 Page 14

security and data management; logging; and customization); and

(iii) includes standard reports that can be run using flexible parameters.

h. Mobile Report Entry (MRE):

(1) The MRE is a field reporting system capable of off-line report entry. The MRE offers transparent integration with the RMS in a mobile environment.

(2) The MRE has been configured so members report writing policies are enforced. Configuring the MRE (for example, hiding fields, making certain fields mandatory, defaulting field values, writing cue card help for report types, etc.), improves uniformity .

(3) Police officers shall complete numerous prefill screens using MRE and will transfer reports to the RMS through the MDT over a data network or File Transfer Protocol (FTP) via desktop.

(4) A separate data transcription application in the RMS is provided to transfer the information entered on the MRE to the RMS.

i. Mobile Data Terminals (MDT):

(1) Mobile computers are to be used for legitimate police business only.

(2) At no time, will users attempt to disable, remove, or alter components of the MDT hardware, including the casing of the laptop or the hard drive of the computer.

(3) Only authorized software may reside or run on mobile computers. Unauthorized software programs or files are prohibited. Authorized software may not be manipulated or altered. Modifying computer settings is prohibited.

CIDDD Exhibit P-0024 Page 15

(4) At the beginning of the shift, employees shall check the MDT while completing their routine vehicle checks. Damaged equipment must immediately be reported to a supervisor.

(5) Employees shall log onto the assigned MDT and shall remain active on the system for the entire shift.

(6) The MDT shall not be used to access or attempt to access the internet.

(7) No food, beverage or any other substance that may cause damage, will be placed on or near the MDT.

(8) Only the provided stylus pen or clean finger may be used to operate the touch screen. Use of any other object to activate the touch screen is prohibited, as it may scratch or otherwise damage the screen display.

(9) Laptop screens should be cleaned with a soft, clean cloth, such as a micro fiber cloth. Use of cleaning solvents and liquid-based products on the computer is prohibited, as they often cause hazing or damage to the screen.

(10) All vehicles equipped with MDTs shall be locked whenever unoccupied. In the event that an officer leaves her/his vehicle or has a citizen remaining in the car, the MDT will be placed in a screen-downed position and the officer will ensure the silent patrolman is locked and secure.

(11) MDTs should be removed from any vehicle which is anticipated to be out of service. The MDT can be forward to the RNC/OCIO office, RNC Information Services, or RNC Facilities and Assets.

(12) If an MDT computer or modem is discovered to be lost or stolen, this shall be reported to the RNC/OCIO office or RNC Information Services Division.

(a) The RNC/OCIO office or RNC Information Services Division

CIDDD Exhibit P-0024 Page 16

shall take the necessary steps to render network access inaccessible, of the lost or stolen device.

11.0 Data Management and Applications

11.1 Requests to access any of the RNC's applications shall be submitted by electronically completing the **Online Request for Network Accounts and/or Computer Equipment Form**.

11.2 Approval is subject to the RNC/OCIO Chart of Authorities.

11.3 The following is a listing of RNC applications and responsible Divisions.

Application Name	Short Description	Responsible Division
RNC ARMORY Inventory System AM Number 119001	Tracks the firearms and ammunition stored and issued by the Range Master at the RNC.	Support Services
Cost Recovery Database AM Number 119005	Tracks the receipt and processing of Applications for Police Checks, Towing, Fingerprinting, Document Disclosure and Accident Reports.	Finance & Information Services
RNC Digital Mug Shot AM Number 119009	Collects client photos and demographic information and court disposition. Produces paper C216 for submission to Federal system.	Identification
HR Training Database AM Number 119020	Records personnel participation in training courses throughout the province. Also records any cost associated with the training.	Training
RNC Offender Sign In Tracker AM Number 119030	Application to record when persons released on an undertaking or recognizance are reporting to the police as ordered by court.	Operational Support Services - TRC
Resource Utilization System (RUS): RNC AM Number 119047	Used by the RNC Finance Division to record leave information, work schedule, overtime accrued, leave related payments for staff.	Finance
Use of Force Training Database AM Number 119059	Records police officers' participation in Use of Force training.	Training
RNC File Sign Out Portal AM Number 119082	The system is used for the File Sign In/Sign Out and File Archives applications.	Information Services
TRIM - Document Management - RNC - Evidence Management AM Number 119086	TRIM implementation for evidence management at the Royal Newfoundland Constabulary.	Information Services

Application Name	Short Description	Responsible Division
RNC MOBL AM Number 119087	A web application designed for a Blackberry. Used by the RNC Patrol Officers to access the Motor Registration Division Database during routine roadside duties.	Information Services
E Disclosure AM Number 119088	The E Disclosure application is a web interface that integrates with TRIM (at the RNC), to prepare cases for electronic disclosure	Information Services
RNC TIU Inventory System AM Number 319096	Used by the Technical Investigation Unit at the RNC for the purpose of inventory management. It is a scaled down, simplified version of the RNC Armory System.	Criminal Investigation Division
Royal Newfoundland Constabulary (RNC) Mobile Data Terminals (MDT) AM Number 319105	The Mobile Data Terminal (MDT) application includes all of the physical infrastructure and software which is required to allow police officers in the field to communicate and send data securely back to RNC headquarters.	Information Services
GNL Static Website - www.rnc.gov.nl.ca - Royal Newfoundland Constabulary & RNC Intranet AM Number 319107	This is the official websites for the Royal Newfoundland Constabulary (RNC).	Strategic Planning & Research
Digital Recording System (RNC) COMLOG AM Number 119011	This "off-the-shelf" system is used in all Communications Centres to record the audio of all designated telephone lines..	Operational Support Services - Communications
Integrated Constabulary Automated Nerowrk (ICAN) AM Number 119021	Computer Aided Dispatch (CAD), Records Management System (RMS), Mobile Report Entry (MRE) are modules that reside within ICAN.	Information Services & Operational Support Services - Communications
RNC Report Warehouse(ICAN)(RNCRW) AM Number 119024	Data extracted from CAD & RMS systems used for statistical and Quality Assurance Reports.	Information Services
Livescan	Enables the RNC to submit fingerprints electronically to CCRTIS	Identification & Information Services
RCMP supported applications access through the Constabulary network		
PIRS / CPIC / ACIIS AM Number 119040	National Records Management System and system used to share police information.	Information Services & Intelligence and Organized Crime Unit

CIDDD Exhibit P-0024 Page 18

Application Name	**Short Description**	**Responsible Division**
GNL supported applications access through the RNC network		
MRD	The Motor Registration Division's (MRD) database application is used to query for license and other driver/vehicle information.	Information Service & Intelligence and Organized Crime Unit
IPCIS	Integrated Provincial Court Information System is used to query court information	Information Services
FMS	Financial Management System	Finance Division