1.0 REFERENCES

1.1. Republic Act No. 11032 or the Ease of Doing Business and Efficient Government Service Delivery Act of 2018;
1.2. Section 2 of the Declaration of Policy of RA No. 8792 or the Electronic Commerce Act of 2000;
1.3. Section 2 of RA No. 10175 or the Cybercrime Prevention Act of 2012;
1.4. DICT MC No. 2015 – 002 dated April 27, 2015, re: Prescribing the GovMail Service Guidelines for Philippine Government Agencies;
1.5. Clause 8.1. ISO 9001:2015, Re: Operational Planning and Control;
1.6. DILG DO No. 2018-648 dated July 2, 2018, Re: Activation of the DICTM of the BJMP;
1.8. Approved BJMP Information System Strategic Plan (ISSP) 2021 to 2023; and

2.0 RATIONALE

The Jail Bureau recognizes the importance of electronic mail (e-mail) system on its operation and the delivery of effective and efficient service to the general public. Its level of importance is again recognized during these challenging times brought about by the COVID-19 pandemic where most have adopted/shifted into online transactions. Parallel with speed and convenience in undertaking transactions is the salience of minimizing risks from either intentional or unintentional misuse.

Not all BJMP personnel have an issued official e-mail account, hence, they use third-party e-mail services such as Gmail or Yahoo mail, which pose risks on the origins and links of online transactions. Having a BJMP official e-mail account shows a corporate identity by using the agency domain in a digital world. It gives value to the operations giving it credibility and weight, particularly in our online transactions.

Alongside the adoption or use of e-mail services is the responsibility to ensure the safety and security of information and other official communications using the BJMP e-mail service. Hence, the adoption of a government policy is necessary to

Prepared by:

RAY XAVIER L TRISTEZA
Jail Senior Inspector
Chief, ICT Plans and Programs Division, DICTM

Reviewed by:

DENNIS U ROCAMORA, CESE
Jail Chief Superintendent
Deputy Chief for Operations of the Jail Bureau
Quality Management Representative

Approved by:

ALLAN S IRAI, CESE
Jail Director
Chief, BJMP

"Changing Lives, Building a Safer Nation"
best fit the needs of the BJMP organization to ensure that its e-mail service does not infringe on the rights of BJMP officials and employees, clients, and the public; should not be used contrary to prohibited laws, rules, and regulations; and will not legally compromise the BJMP or the government as a whole.

3.0 OBJECTIVE

This policy is developed to ensure the establishment of secure and appropriate controls for e-mail communications.

Electronic Mail (E-mail) refers to the exchange of digital messages through a network using software and servers. It is designed to improve services to customers, enhance timely internal communications, promote reliable, accessible information and reduce paper work. Further, an e-mail system has different risks compared to paper-based communications.

4.0 SCOPE / COVERAGE

4.1. This circular covers the policy guidelines on use and issuance of official e-mail accounts to the BJMP offices, active and permanent personnel and staff. It sets guidelines and prohibitions as well as on the use of the BJMP e-mail system and provision of corresponding administrative sanctions.

4.2. EXCLUSION

This policy excludes the specific guidelines for sending large file attachments, mailing list, distribution list or group list, that needs to be distributed and made accessible to a set of people indicated in the mailing list, distribution list, and group list, that does not have its own account inbox.

5.0 DEFINITION OF TERMS

5.1. **Account Holder** refers to one or more of the following, (a) BJMP Employees, and (b) individuals authorized by the Chief, BJMP to use the BJMP e-mail for a specific purpose and duration.

5.2. **Attachments** are textual, graphical, visual or executable files that are attached in the e-mail messages.

5.3. **Bulk Mail** is an e-mail message sent to three (3) or more recipients.

5.4. **Chief Information Officer (CIO)** is another term which refers to the Director for Information and Communications Technology Management (DICTM) of the Jail Bureau who is responsible for information systems planning and implementation of BJMP ICT strategic direction in ICT governance.

5.5. **Counterfeit or Forged E-mails** are e-mail accounts that make use or may contain invalid or forged headers, invalid or non-existent domain names or other names that are deceptive.

5.6. **Electronic Mail (E-mail)** refers to the exchange of digital messages through a network using software and servers.

5.7. **E-mail Account Administrator** is a person in-charge of the agency’s e-mail account administration.

"Changing Lives, Building a Safer Nation"
5.8. **Employees** refer to all current employees of the BJMP whose appointments are active and permanent.

5.9. **Hypertext Transfer Protocol Secure (HTTPS)** is a communication protocol for secure communication over a computer network.

5.10. **Internet Message Access Protocol (IMAP)** is a protocol for e-mail retrieval and storage.

5.11. **Internet** is a system of linked computer networks, global in scope, that facilitates data communications services, such as remote log-in, file transfer, and electronic mail, and newsgroups. It is a way of connecting computers and computer networks, greatly extending the reach of each participating system.

5.12. **Log-in** is an operation that enables the account holder to access the mailbox, such as the act of typing information, which consists of the username and password or other mechanisms to gain access to the BJMP e-mail service.

5.13. **Log-out** is an operation that terminates access to the BJMP e-mail service.

5.14. **Mailbox** is a functional unit that contains stored messages for a specific account holder.

5.15. **Password** is a string of characters that is used as authentication to access BJMP e-mail service.

5.16. **Personnel or Employee Account** refers to an e-mail account provided or issued to a personnel or employee using the domain @bjmp.gov.ph.

5.17. **Spam** refers to electronic junk mail or an unsolicited bulk e-mail received that is unrelated to work and not otherwise justified.

### 6.0 PROCEDURES/DETAILS/ GUIDELINES

6.1. **POLICY STATEMENT**

6.1.1. Official e-mail accounts shall be provided to employees of the BJMP who shall require communicating through e-mail in transacting business for the Jail Bureau. There should be official e-mail accounts for authorized employees of the BJMP, i.e., e-mail ID based on designation. Whenever an officer/employee gets transferred or separated from the service, it shall be the responsibility of the concerned office to get password changed or reported to the Directorate for Personnel and Records Management (DPRM) or the Directorate for Information and Communications Technology Management (DICTM).

6.1.2. Decision to provide e-mail accounts to non-employees is the discretion of the BJMP management.

6.1.3. Information created, sent, or received via BJMP e-mail system, including messages and electronic files, are considered properties of the BJMP.

6.1.4. The BJMP management shall have access to all e-mail messages when required to present to law enforcement agencies or third parties without consent of the e-mail user.

("Changing Lives, Building a Safer Nation")
6.1.5. E-mails and electronic messages shall be protected from unauthorized access, alterations, and denial of service.

6.1.6. Users shall abide by copyright laws, ethical rules, and other applicable laws while using BJMP e-mail system.

6.1.7. Users shall exercise sound judgment when distributing messages. Client-related messages shall be guarded and protected.

6.1.8. Users shall not use the e-mail facility for unauthorized use. E-mail accounts shall be established and used for official purposes only to provide individual employees with a faster, efficient, and transparent communication with other government employees, offices, and the general public.

6.1.9. E-mail messages sent to the name of the BJMP shall be consistent with BJMP policies.

6.1.10. The e-mail attachments with extensions, such as, “exe,” “scr” and “vbs,” etc., are considered unsafe and are potentially harmful, thus, it shall be blocked for security reasons.

6.1.11. Re-directions/auto-forwarding of e-mails from BJMP e-mail accounts to any external e-mail accounts shall be prohibited.

6.1.12. The e-mail system shall protect the right to confidentiality of users.

6.1.13. Use of BJMP e-mail system to solicit for commercial or personal benefit without appropriate authorization shall be prohibited.

6.1.14. E-mails sent outside the organization shall have an appropriate disclaimer attached. (Attached under 6.2.9.1 standard disclaimer)

6.1.15. Mailbox not accessed for more than six (6) months period shall be blocked.

6.1.16. Users shall report e-mail security incidents in accordance with the Information System incident management policy.

6.1.17. E-mail exchange server should be periodically updated, and necessary security patches should be installed.

6.1.18. In case accounts contain critical information, advanced log-in techniques such as Multi-lingual Image based Virtual Keyboard shall be implemented for accessing e-mail.

6.1.19. Links to external sites on e-mail should not be allowed to open directly. Links may contain harmful executable programs, spam, phishing links, or inadequate/restricted websites.

6.1.20. Violation of e-mail policy shall be subjected to disciplinary action.

6.1.21. All official electronics communications shall be executed through BJMP e-mail accounts.

"Changing Lives, Building a Safer Nation"
6.2. GUIDELINES AND PROCEDURES

6.2.1. Office or Non-Personnel Account

6.2.1.1. The BJMP Office or non-personnel accounts shall be provided to the offices of the National Headquarters, Regional Offices, Provincial Jail Administrators Offices and to the district, city and municipal jails. This shall be used as means of official communications within the Jail Bureau, with other government agencies and the general public.

6.2.1.2. The Chief, Administrative Officers of concerned offices shall be responsible for the assignment, request for creation, transfer, and deactivation of e-mail account from the DICTM. Upon approval, the e-mail account shall be created by the designated e-mail account administrator. Likewise, upon transfer of office administrator, the Chief Administrative Officer shall request the transfer of credentials to the succeeding administrator or their deactivation by the DICTM.

6.2.1.3. The office or non-personnel accounts shall be published in the BJMP website in compliance with Republic Act No. 11032 or the Ease of Doing Business and Efficient Government Service Delivery Act of 2018.

6.2.2. Personnel or Employee Account

6.2.2.1. The Personnel or Employee account shall be established and used for official purposes only to provide individual personnel or employee with faster, efficient, and transparent communication means with other government employees, offices, and the general public.

6.2.2.2. The personnel or employees shall submit to the DPRM/PRMD a request for creation of their official e-mail accounts.

6.2.2.3. The DPRM/PRMD shall prepare a list of personnel or employees who have submitted request for official BJMP e-mail accounts and shall submit the same to DICTM for confirmation.

6.2.2.4. Upon confirmation of the DICTM, the e-mail administrator shall create the personnel or employee official e-mail account.

6.2.2.5. The e-mail administrator shall provide instructions to the personnel or employee on how to access the e-mail account. A copy of policy shall be provided to the concerned personnel or employee.

6.2.2.6. Before requesting new e-mail accounts from the DICTM, the e-mail account administrator must issue certification that 100% of e-mail accounts are active or have been accessed for at least one week.

6.2.3. E-mail Naming Convention

The naming convention for Office and Employee account shall be observed, as follows:

6.2.3.1. An e-mail shall include the name of directorate/office/division/section/unit or project of the Jail Bureau, followed by the domain @bjmp.gov.ph. (See Annex C)

"Changing Lives, Building a Safer Nation"
6.2.3.2. For employee's e-mail account, the general format of e-mail address shall include the first name or nickname in which the personnel or employee is known, followed by period (.) and the last name, followed by the domain.

Example: juan.delacruz@bjmp.gov.ph

6.2.3.3. In case the employee has the same first name and last name with another person, the employee hired first shall follow 6.2.3.2 and the succeeding employees shall have the following e-mail address naming options.

Option 1: juanb.delacruz@bjmp.gov.ph
Option 2: jbautista.delacruz@bjmp.gov.ph
Option 3: jb.delacruz@bjmp.gov.ph

6.2.4. Privacy and Monitoring

Relative to Section 2 Presidential Decree No. 1445 or Government Auditing Code of the Philippines, all data, information and communications sent, received or archived through the BJMP official e-mail address belong to the government. It shall be understood that in the use of BJMP e-mail service, all messages or files sent through the BJMP e-mail service may be accessed by the employees' superior, head of agency and other authorized officer, for work, administration, or disciplinary purposes.

6.2.5. E-mail Archiving, Backup and Retention

All official e-mails shall be archived in accordance with mechanisms and policies to be issued by the Jail Bureau as part of Agency Records Disposition Schedule in accordance with the rules and regulations set by the National Archives of the Philippines.

6.2.6. Password

6.2.6.1. Account holders shall be responsible of their respective passwords. It should not be written down, stored or shared with other persons.

6.2.6.2. Ten (10) consecutive failed log-in attempts within (10) minutes shall result in the automatic e-mail account lock-out for thirty (30) minutes.

6.2.6.3. Passwords must have a specified minimum length of at least eight (8) characters comprised of a combination of, a) uppercase letters, b) lower case letters, c) numbers, and d) special characters or symbols, such as, = ? < > @ # $ * and !.

6.2.7. Suspension or Termination

6.2.7.1. Termination or suspension of personnel or employee e-mail accounts shall be implemented in the following instances: a) in cases of disciplinary action; b) transfer of account holder from BJMP to another agency of the government; c) retirement; or d) separation from the service.

"Changing Lives, Building a Safer Nation"
6.2.7.2. In case of suspension or termination of e-mail account, the DPRM shall prepare a report stating that the account holder can no longer use the official e-mail address, either permanently or temporarily, as the case may be. The report shall state the reason for such suspension or termination, which shall be submitted to the DICTM for evaluation.

6.2.7.3. In every instance of suspension or termination of e-mail account, the DICTM shall direct the account administrator to suspend or terminate the e-mail account of the concerned personnel or employee.

6.2.7.4. When a personnel or employee resigns or retires, a 30-day notice shall be given to the concerned personnel or employee before the account holder’s access to BJMP official e-mail address may be terminated.

6.2.7.5. When personnel or employee is separated from the service for a cause, access to his/her official e-mail account shall be immediately blocked. After 30 days, the e-mail account shall be automatically terminated.

6.2.8. Spam, Counterfeit, or Forged E-mail

In the occurrence of Spam, Counterfeit, or Forged e-mails, the account holder shall send a copy of spam, counterfeit or forged e-mail to the account administrator for immediate investigation. Report shall contain the following information:

6.2.8.1. Subject line “SPAM” together with the subject of the Spam or Counterfeit e-mail (ex. SPAM: Chain Letter).

6.2.8.2. The e-mail address of the sender of the Spam or Counterfeit e-mail should be in the body of the mail.

6.2.8.3. The complete headers must be sent to the e-mail account administrator. This is done by sending the entire e-mail as an attachment.

6.2.9. Standard E-mail Signature and Disclaimer

The Jail Bureau shall use a standard e-mail signature using the following format:

Complete Name of Personnel / Employee  
Position / Designation  
Unit / Section / Division / Office  
Complete Agency Address  
Telephone / Fax Number  
www.bjmp.gov.ph

6.2.9.1. All BJMP e-mail accounts shall use a standard disclaimer, to wit:

“The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed, and other parties authorized to receive it. It may contain confidential or legally privileged communication. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or taking any

“Changing Lives, Building a Safer Nation”
action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this e-mail and immediately delete it from your system. Opinions contained on this e-mail or any of its attachments do not necessarily reflect the opinions of the Jail Bureau.”

6.3. ACCEPTABLE USE OF THE BJMP E-MAIL SERVICE

6.3.1. As a rule, any e-mail sent using the BJMP e-mail service is permitted for as long as the same is used in the performance of official duties and responsibilities. When using the BJMP e-mail service, the account holders shall act professionally and shall be bound by the provisions of the Code of Conduct and Ethical Standards for Public Official and Employees (RA No. 6713).

6.3.2. All e-mails sent through the BJMP e-mail service not related to the performance of official duties and responsibilities shall fall under Section 6.4, or the Prohibited Use of BJMP e-mail Service and may be subjected to administrative disciplinary actions.

6.3.3. Messages sent through BJMP e-mail service shall follow the Bureau’s communication flow, protocol, and policies.

6.3.4. E-mail account holders, in creating e-mail, shall observe e-mail etiquette. (Annex A)

6.4. PROHIBITED USE OF BJMP E-MAIL SERVICE

6.4.1. No e-mail shall be sent through BJMP e-mail service for purposes outside the performance of official duties and responsibilities. It shall not be used to send out containing derogatory, defamatory, insulting, jokes, rumors, gossips, opinions, abusive, or libelous information about any other BJMP’s Employee, client, associate, or any other person not related in the performance of official duties and responsibilities.

6.4.2. E-mail account holders shall be prohibited from accessing, copying, or deleting the e-mail of another account holder without the consent of the latter.

6.4.3. Account holders shall not disclose their passwords to other persons unless the Jail Bureau requires it.

6.4.4. The BJMP e-mail service shall not be used for the creation or distribution of messages that are disruptive or offensive to other persons, including offensive comments and statements about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs, and practices, political beliefs, or national origin.

6.4.5. The BJMP e-mail service shall not be used for personal or commercial purposes and for the promotion of business or other matters outside of the Jail Bureau or the government.

6.4.6. As a rule, sending of bulk mail shall be prohibited unless such bulk mail is formally solicited. Users should send e-mail messages and copies thereof only to those with legitimate need to read the message.

“Changing Lives, Building a Safer Nation”
6.4.7. Overloading unnecessarily or frivolously the e-mail system (e.g., chain mail, spamming, executable graphics and/or programs and junk mail) is not allowed.

6.4.8. Enclosing information that is harmful to BJMP operations and reputation, as well as, its employees.

6.4.9. Attaching files in the e-mail message is discouraged. File attachments shall be implemented through separate sending service.

6.4.10. Any document covered by Memorandum Circular No. 78 dated August 14, 1968, re: Security of Classified Matter in Government Departments and Instrumentalities, as amended by Memorandum Circular 196 dated July 19, 1968, shall not be sent using the BJMP official e-mail until specific guidelines are issued by the National Security Council, Department of National Defense, or the Office of the President for classified, confidential or other e-mail messages of risk to National Security.

6.4.11. The use of materials, procedures, devices, or technologies that will enable the unauthorized access to BJMP e-mail system is prohibited.

6.4.12. Authorized users are prohibited from using their respective official e-mail accounts in registering or joining Social Networking Sites and other list groups for personal use in nature.

6.5. ADMINISTRATION, OPERATION AND MAINTENANCE OF BJMP E-MAIL SYSTEM

6.5.1. The administration, operation, and maintenance of the BJMP e-mail system, including the servers, shall be the responsibility of the DICTM to ensure the reliability, integrity, and efficiency of the system.

6.5.2. The DICTM shall develop the necessary rollout plan for the BJMP e-mail system for all its personnel and shall formulate tools to monitor its implementation in coordination with the DPRM.

6.5.3. The DICTM, in coordination with the DPRM, shall come up with the needed resources to ensure a smooth and successful implementation of the BJMP e-mail system.

6.6 RESPONSIBILITIES

6.6.1. DICTM

6.6.1.1. Shall establish the official naming convention for e-mail addresses;

6.6.1.2. Shall provide maintenance and technical support during service downtimes or disruptions, including disruptions affecting related services;

6.6.1.3. Shall provide system updates, patches, bug fixes, and other processes or operations affecting the BJMP e-mail service;

"Changing Lives, Building a Safer Nation"
6.6.1.3 Shall provide system updates, patches, bug fixes, and other processes or operations affecting the BJMP e-mail service;

6.6.1.4 Shall orient all BJMP personnel on the acceptable and prohibited use of BJMP e-mail service;

6.6.1.5 Shall provide administrator and account management support which is limited only on account management, creation, deletion, and editing of e-mail accounts;

6.6.1.6 Shall monitor the e-mail service provisions;

6.6.1.7 Shall regulate and conduct the necessary investigation on matters relating to antispam and counterfeit or forged e-mail; and

6.6.1.8 Shall issue other policy documents relating to the e-mail service, as may be necessary.

6.6.2 DPRM

6.6.2.1 Shall communicate with the DICTM on administrative matters relating to the BJMP e-mail service;

6.6.2.2 Shall ensure that the BJMP e-mail is provided to government employees who need it;

6.6.2.3 Shall ensure that official e-mail accounts are posted in accordance with the RA No. 11032;

6.6.2.4 Shall ensure that the e-mail addresses adhere to the provisions of the approved e-mail naming convention by the DICTM;

6.6.2.5 Shall store and maintain all relevant information of the BJMP e-mail account holders, whether personal or technical, and to be able to reproduce such information as may be required;

6.6.2.6 Shall ensure that all agency e-mail account holders have undergone the orientation on the use of e-mail system conducted by the DICTM;

6.6.2.7 Shall prepare a detailed report in case of suspension or termination of an e-mail account;

6.6.2.8 Shall ensure that the BJMP e-mail account holders agree and acknowledge to the terms and conditions set under the policy on the use of BJMP e-mail system; and

6.6.2.9 Shall designate two personnel who will act as the BJMP e-mail account administrator and alternate.

6.6.3 E-mail Account Administrator:

6.6.3.1 Email Account Administrator pursuant to 6.6.2.9 shall be designated from DPRM, as primary and DICTM, as alternate account administrators.

"Changing Lives, Building a Safer Nation"
6.6.3.2 Shall implement the e-mail policy consistently and uniformly;

6.6.3.3 Shall provide additional accounts for new and approved personnel, as well as non-personnel accounts and distribution lists recommended by the DICTM and approved by the Chief, BJMP;

6.6.3.4 Shall handle first level e-mail support for all BJMP employees which includes, but not limited to inquiries on e-mail account, password changes, account status modification, including activation, locking and closing, and account detail updates;

6.6.3.5 Shall escalate other support cases to the DICTM;

6.6.3.6 Shall disseminate information, announcements, and notices from the DICTM to all employees;

6.6.3.7 Shall submit the usage statistics, administration activity monitoring logs, and compliance monitoring report every month to the DICTM;

6.6.3.8 Shall deactivate and archive the e-mails of the authorized users who have transferred, resigned, retired, those separated from the service, or those whose e-mail privilege has been suspended; and

6.6.3.9 Shall act as one of the signatories to the Employee Clearance required for resigning, retiring, or separated employees.

6.6.4 Authorized users

6.6.4.1 Shall sign and acknowledge the orientation on the policy on the use of BJMP e-mail system;

6.6.4.2 Shall be accountable for e-mails emanating from their account;

6.6.4.3 Shall read e-mail service policy and confirm to the e-mail account administrator that he/she has read and understood this policy and will abide by it;

6.6.4.4 Shall read email service policy to be given physically or by softcopy by the e-mail account administrator and confirm that he/she has read and understood this policy and will abide by it by signing the given hardcopy or softcopy policy.

6.6.4.5 Shall make use of e-mail service as a means of communications within BJMP offices and employees, government offices, and the general public;

6.6.4.6 Shall keep their respective passwords secure;

6.6.4.7 Shall log out of their respective e-mail accounts and refrain from leaving the account unattended;

6.6.4.8 Shall adhere to BJMP e-mail naming convention (See 6.2.3 for E-mail Naming Convention);

"Changing Lives, Building a Safer Nation"
6.6.4.9 Shall report any occurrence of spam, counterfeit, or forged e-mail to the e-mail administrator (See 6.2.8 for Spam, Counterfeit or Forged E-mail); and 

6.6.4.10 Shall report immediately any instance of violation of this policy to their immediate supervisor.

6.7 ENFORCEMENT

Any reported abuse, or inappropriate use of BJMP e-mail service shall be subjected to disciplinary action in accordance with the BJMP Administrative Machinery and the Civil Service Commission's prescribed Uniform Rules on Administrative Cases (See Annex B for list of possible Violations and Equivalent Administrative Offenses and the Sanctions).

Above administrative actions and proceedings shall be without prejudice to the filing in court of any other applicable charges that may be filed by the aggrieved party.

6.8 SYSTEM AUDIT

The BJMP e-mail system shall be audited once a year by a Certified Information Security Auditor (CISA) using applicable and relevant standards. For this purpose, the BJMP shall include the development of training and certification programs for CISA or Certified Information Security Officer (CISO) for its personnel assigned at the DICTM.

6.9 TRANSITORY PROVISION

The DICTM shall act as the e-mail service administrator until the designation of an e-mail administrator from the DPRM proficient to take over the DICTM as the alternate administrator.

7.0 MONITORING PROCEDURE/ TOOL

This policy shall be reviewed and evaluated by the DICTM once a year based on its effectiveness, cost to maintain, and impact on technical processes. This policy may be revised anytime based on the needs and newly discovered risk/s, security incidents involving e-mail service or major changes with the BJMP organizational setup or information system.

8.0 FINANCIAL CLAUSE

The BJMP shall allocate funds for the implementation of this Circular. Issuance of official e-mail account, user's orientation, and technical trainings shall be programed and included in the annual budget proposal viz-a-viz the annual recruitment program.

9.0 SEPARABILITY CLAUSE

In the event that any provision or part of this policy be declared unauthorized or rendered invalid by a competent authority, the remaining provisions shall remain valid and effective.

"Changing Lives, Building a Safer Nation"
10.0 REPEALING CLAUSE

All policies, directives, and other issuances which are inconsistent with the provisions of this Circular are hereby repealed, amended, rescinded, or modified accordingly.

11.0 EFFECTIVITY

This Memorandum Circular shall take effect after 15 days from the filing thereof with the UP Law Center (UPLC)- Office of the National Administrative Register (ONAR) in consonance with Sections 3 and 4 Chapter 2 Book VII of Executive Order Number 292, otherwise known as Revised Administrative Code of 1987, as amended.

12.0 ANNEXES

Annex A. Proper E-mail Etiquette  
Annex B. List of Violations and Its Equivalent Administrative Offense and CSC Sanctions  
Annex C. List of BJMP Office E-mail Address

Prepared by:

RAY XAVIER L TRISTEZA  
Jail Senior Inspector  
Chief, ICT Plans and Programs Division, DICTM

Reviewed by:

DENNIS U ROCAMORA, CESE  
Jail Chief Superintendent  
Deputy Chief for Operations of the Jail Bureau  
Quality Management Representative

Approved by:

ALLAN S IRAL, CESE  
Jail Director

Chief, BJMP

"Changing Lives, Building a Safer Nation"
Annex A. ELECTRONIC MAIL ETIQUETTE

1. Be sure to include a subject line.
2. Consider using BCC to keep e-mail address private or to ensure that the "To:" area of the message remains a small size.
3. Write clear and concise message/s.
4. Write short sentences.
5. Avoid double spacing your message as e-mail requires recipients to scroll through a message without the benefit of highlighting or marking the message as one might on a printout.
6. Use a descriptive subject line.
7. Avoid using capital letters for all text.
8. Avoid using colored fonts.
9. When replying to a message, consider deleting part of the original message to save space on the screen. Retain only the part of the sender's message to which you are responding.
10. Avoid using the Reply To All function as this sends your response to all recipients of the e-mail.
11. Avoid acronyms because not everyone will know their meaning.
12. Use proper grammar and conduct a spell check of your message.
13. Use simple fonts because computers may have a limited number of font available for e-mail use. Using a small or compact font keeps the message in a more confined area.
14. Be specific. State terms and conditions clearly to avoid miscommunication, especially when providing information about times, places or people.
15. Leave the address field blank and fill it out last, to avoid sending unchecked or hastily written messages.
16. Do not use unnecessary punctuations.
17. Do not use text messaging shortcuts.
18. Avoid emoticons.
19. Never use slang languages.
22. Never reply to a spam.
23. Be cautious when sending attachments.
25. Never open e-mails not intended for you or, coming from unknown sender.

"Changing Lives, Building a Safer Nation"
## Annex B. List of Violations and Equivalent Administrative Offenses and Sanctions

<table>
<thead>
<tr>
<th>Violations</th>
<th>Equivalent Administrative Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commercial Use</strong> – Use of BJMP ICT resources for commercial purpose and product advertisement for personal profit.</td>
<td>Dishonesty / Grave Misconduct</td>
</tr>
<tr>
<td><strong>Religious Lobbying</strong> – Use of BJMP ICT resources for religious lobbying.</td>
<td>Conduct Prejudicial to the Best Interest of the Service</td>
</tr>
<tr>
<td><strong>Political Lobbying</strong> – Use of BJMP ICT resources for political lobbying.</td>
<td>Engaging directly or indirectly in partisan political activities by one holding non-political office</td>
</tr>
<tr>
<td><strong>Copyright Infringement</strong> – Reproduction, duplication or transmission of copyrighted materials.</td>
<td>Dishonesty</td>
</tr>
<tr>
<td><strong>Criminal Use</strong> – Using the resources for criminal use.</td>
<td>Grave Misconduct</td>
</tr>
<tr>
<td><strong>Stealing</strong> – stealing information resources both hardware or software or any part of the network resource.</td>
<td>Grave Misconduct</td>
</tr>
<tr>
<td><strong>Concealing Access</strong> – concealing one’s identity or masquerading as another user to access the information resource, send/receive, process, modify or store data on the BJMP ICT resources.</td>
<td>Grave Misconduct</td>
</tr>
<tr>
<td><strong>Password Disclosure</strong> – disclosure of user password protected account or making the account available to others without the permission of the e-mail system administrator.</td>
<td>Grave Misconduct</td>
</tr>
<tr>
<td><strong>Unlawful Messages</strong> – use of electronic communication facilities (e.g. e-mail, talk, chat or system with similar functions) to send fraudulent, harassing, obscene, threatening or other offensive message.</td>
<td>Simple Misconduct</td>
</tr>
<tr>
<td><strong>Offensive Prohibited Materials</strong> – use of computers, printers, electronic mail, data network, and other related resources to produce, disseminate, store or display materials which could be considered offensive, pornographic, racially abusive, libelous or violent nature.</td>
<td>Simple Misconduct</td>
</tr>
<tr>
<td><strong>Prohibited Materials</strong> – using or encouraging the use of materials that includes instructions to gain unauthorized access.</td>
<td>Simple Misconduct</td>
</tr>
<tr>
<td><strong>Unauthorized reading of e-mail or private communications of other users, unless otherwise requested to do so by said user.</strong></td>
<td>Simple Misconduct</td>
</tr>
</tbody>
</table>

"Changing Lives, Building a Safer Nation"
<table>
<thead>
<tr>
<th>Misrepresentation in sending e-mail messages.</th>
<th>Falsification of official document or Simple Misconduct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not cooperating with any investigating process in line with computer, network, or system abuse.</td>
<td>Violation of Reasonable Rules and Regulations</td>
</tr>
<tr>
<td>Disclosure of BJMP Confidential Information – Transmission of information without authority and/or proper security clearance.</td>
<td>Disclosing or misusing confidential or classified information officially known to him by reason of his office and not available to the public, to further his private interest or give undue advantage to anyone or to prejudice to the public interest</td>
</tr>
<tr>
<td>Access to lewd sites and/or materials – a user shall not view, transmit, retrieve, save or print any electronic file, image or text which may be deemed sexually explicit or pornographic.</td>
<td>Violations of Reasonable Rules and Regulations</td>
</tr>
</tbody>
</table>

"Changing Lives, Building a Safer Nation"
<table>
<thead>
<tr>
<th>ADMINISTRATIVE OFFENSE</th>
<th>SANCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engaging directly or indirectly in partisan political activities by one holding non-political office</td>
<td>1st Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Falsification of official document</td>
<td>1st Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Grave Misconduct</td>
<td>1st Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Dishonesty</td>
<td>1st Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Disclosing or misusing confidential or classified information officially known to him by reason of his office and not available to the public, to further his private interest or give undue advantage to anyone or to prejudice to the public interest</td>
<td>1st Offense – **Suspension for six (6) months and one (1) day to one (1) year; 2nd Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Conduct Prejudicial to the Best Interest of the Service</td>
<td>1st Offense – **Suspension for six (6) months and one (1) day to one (1) year; 2nd Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Simple Misconduct</td>
<td>1st Offense – **Suspension for one (1) month and one (1) day to one (1) year; 2nd Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Violation of existing Civil Service Law and Rules of Serious of Nature</td>
<td>1st Offense – **Suspension for one (1) month and one (1) day to one (1) year; 2nd Offense – <strong>Dismissal</strong></td>
</tr>
<tr>
<td>Violation of Reasonable Office Rules and Regulations</td>
<td>1st Offense – **Reprimand; 2nd Offense – Suspension for one (1) month and one (1) day to one (1) year; 3rd Offense – <strong>Dismissal</strong></td>
</tr>
</tbody>
</table>

"Changing Lives, Building a Safer Nation"
## ANNEX C. LIST OF BJMP OFFICE E-MAIL ADDRESS

<table>
<thead>
<tr>
<th>No.</th>
<th>Name of Office</th>
<th>E-mail Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Office of the Chief, BJMP</td>
<td><a href="mailto:chief@bjmp.gov.ph">chief@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>2.</td>
<td>Office of the Chief, BJMP2</td>
<td><a href="mailto:chiefbjmp@bjmp.gov.ph">chiefbjmp@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>3.</td>
<td>Deputy Chief for Administration</td>
<td><a href="mailto:dca@bjmp.gov.ph">dca@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>4.</td>
<td>Deputy Chief for Operations</td>
<td><a href="mailto:dco@bjmp.gov.ph">dco@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>5.</td>
<td>Chief Directorial Staff</td>
<td><a href="mailto:cds@bjmp.gov.ph">cds@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>6.</td>
<td>Directorate for Operations</td>
<td><a href="mailto:operations@bjmp.gov.ph">operations@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>7.</td>
<td>Directorate for Comptrollership</td>
<td><a href="mailto:comptroller@bjmp.gov.ph">comptroller@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>8.</td>
<td>Directorate for Health Service</td>
<td><a href="mailto:dhs@bjmp.gov.ph">dhs@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>9.</td>
<td>Directorate for Personnel and Record Management</td>
<td><a href="mailto:personnel@bjmp.gov.ph">personnel@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>10.</td>
<td>Directorate for Human Resource Development</td>
<td><a href="mailto:dhrd@bjmp.gov.ph">dhrd@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>11.</td>
<td>Directorate for Welfare and Development</td>
<td><a href="mailto:dwd@bjmp.gov.ph">dwd@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>12.</td>
<td>Directorate for Information and Communications</td>
<td><a href="mailto:dictm@bjmp.gov.ph">dictm@bjmp.gov.ph</a></td>
</tr>
<tr>
<td></td>
<td>Technology Management</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Directorate for Program Development</td>
<td><a href="mailto:pd@bjmp.gov.ph">pd@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>14.</td>
<td>Directorate for Logistics</td>
<td><a href="mailto:logistics@bjmp.gov.ph">logistics@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>15.</td>
<td>Directorate for Intelligence</td>
<td><a href="mailto:intelligence@bjmp.gov.ph">intelligence@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>16.</td>
<td>Directorate for Investigation and Prosecution</td>
<td><a href="mailto:investigation@bjmp.gov.ph">investigation@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>17.</td>
<td>Information and Communications Technology Service</td>
<td><a href="mailto:ictso@bjmp.gov.ph">ictso@bjmp.gov.ph</a></td>
</tr>
<tr>
<td></td>
<td>Office</td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>Finance Service Office</td>
<td><a href="mailto:finance@bjmp.gov.ph">finance@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>19.</td>
<td>Community Relations Services Office</td>
<td><a href="mailto:crs@bjmp.gov.ph">crs@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>20.</td>
<td>National Executive Jail Officers Office</td>
<td><a href="mailto:nesjo@bjmp.gov.ph">nesjo@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>21.</td>
<td>Chaplaincy Service Office</td>
<td><a href="mailto:chaplain@bjmp.gov.ph">chaplain@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>22.</td>
<td>Legal Service Office</td>
<td><a href="mailto:legal@bjmp.gov.ph">legal@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>23.</td>
<td>Accounting Service Office</td>
<td><a href="mailto:accounting@bjmp.gov.ph">accounting@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>24.</td>
<td>Headquarters Support Service Office</td>
<td><a href="mailto:supportservice@bjmp.gov.ph">supportservice@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>25.</td>
<td>Supply Accountable Office</td>
<td><a href="mailto:supply@bjmp.gov.ph">supply@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>26.</td>
<td>Legislative Liaison Office</td>
<td><a href="mailto:liaison@bjmp.gov.ph">liaison@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>27.</td>
<td>BJMPRO-RI</td>
<td><a href="mailto:bjmpro1@bjmp.gov.ph">bjmpro1@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>28.</td>
<td>BJMPRO-RII</td>
<td><a href="mailto:bjmpro2@bjmp.gov.ph">bjmpro2@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>29.</td>
<td>BJMPRO-RIII</td>
<td><a href="mailto:bjmpro3@bjmp.gov.ph">bjmpro3@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>30.</td>
<td>BJMPRO-CALABARZON</td>
<td><a href="mailto:bjmpro4a@bjmp.gov.ph">bjmpro4a@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>31.</td>
<td>BJMPRO-MIMAROPA</td>
<td><a href="mailto:bjmpro4b@bjmp.gov.ph">bjmpro4b@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>32.</td>
<td>BJMPRO-RV</td>
<td><a href="mailto:bjmpro5@bjmp.gov.ph">bjmpro5@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>33.</td>
<td>BJMPRO-RVI</td>
<td><a href="mailto:bjmpro6@bjmp.gov.ph">bjmpro6@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>34.</td>
<td>BJMPRO-RVII</td>
<td><a href="mailto:bjmpro7@bjmp.gov.ph">bjmpro7@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>35.</td>
<td>BJMPRO-VIII</td>
<td><a href="mailto:bjmpro8@bjmp.gov.ph">bjmpro8@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>36.</td>
<td>BJMPRO-RIX</td>
<td><a href="mailto:bjmpro9@bjmp.gov.ph">bjmpro9@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>37.</td>
<td>BJMPRO-RX</td>
<td><a href="mailto:bjmpro10@bjmp.gov.ph">bjmpro10@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>38.</td>
<td>BJMPRO-RXI</td>
<td><a href="mailto:bjmpro11@bjmp.gov.ph">bjmpro11@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>39.</td>
<td>BJMPRO-RXII</td>
<td><a href="mailto:bjmpro12@bjmp.gov.ph">bjmpro12@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>40.</td>
<td>BJMPRO-CARAGA</td>
<td><a href="mailto:bjmprocaraga@bjmp.gov.ph">bjmprocaraga@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>41.</td>
<td>BJMPRO-BARMM</td>
<td><a href="mailto:barmm@bjmp.gov.ph">barmm@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>42.</td>
<td>BJMPRO-CAR</td>
<td><a href="mailto:bjmprocar@bjmp.gov.ph">bjmprocar@bjmp.gov.ph</a></td>
</tr>
<tr>
<td>43.</td>
<td>BJMPRO-NCR</td>
<td><a href="mailto:bjmproncr@bjmp.gov.ph">bjmproncr@bjmp.gov.ph</a></td>
</tr>
</tbody>
</table>

"Changing Lives, Building a Safer Nation"