D-13442/1

MONTENEGRO

MINISTRY OF FINANCE

CUSTOMS ADMINISTRATION

INFORMATION SECURITY POLICY

TABLE OF CONTENTS

RECORDS OF MODIFICATIONS (DOCUMENT VERSION)

a.	*Version:*	
b.	*Date:*	
c.	*Modification on page:*	
d.	*Modification description:*	
e.	*Requestor of modification:*	

ABBREVIATIONS

MoF	Ministry of Finance
MPA	Ministry of Public Administration
CA	Customs Administration
IS	Information system
INFOSEC	Information security
CIS	Customs Information System
ISP	Information Security Policy
ISA	Information Security Advisor

DEFINITION OF TERMS

- ***Information system*** (IS) is an integrated set of components for collecting, recording, storing, processing and transfer of data.
- ***Information security*** (INFOSEC) entails keeping information confidential, integral and available.
- ***Data*** is information, message or document created, sent, received, recorded, stored or displayed electronically, optically or by similar means, including internet transfer of electronic mail.
- ***Data confidentiality*** implies that data is made available only to persons who have been authorized to access or handle such data.
- ***Data Integrity*** entails maintenance of the existence, accuracy and consistency of data, as well as protection of processes or programs that prevent unauthorized data modification.
- ***Data availability*** means that authorized users may always access data, should a need arise.
- ***Information System Resources*** include
  - **Hardware** – computers and computer equipment, data storage systems, as well as all other technical equipment that supports information system operation
  - **Software** – operating systems, information system monitoring programs, security programs, user programs, database management programs, program development tools, service programs and other programs in the information systems.
  - **Information property** – data in databases, data files, source codes, documentation on information systems and programs, manuals, plans and other information system services.
- ***Security and Standardization Group (02/01-1)*** – Rulebook on Internal Organization and Systematization of Customs Administration. The group was formed as part of the Customs and Information System Sector (02), Department of System Development and Support (02/01).
- ***Information Security Advisor (ISA)*** – *customs employee who is covering the position of an "Customs Senior Advisor I - IT Security Specialist"* within the Security and Standardization Group.

1. PURPOSE

Customs Administration Information Security Policy (ISP) represents an umbrella document which defines leading principles and responsibilities required for the protection of the information system of this institution.

The purpose of ISP is to provide a security framework that will enable protection of CA data from unauthorized access, loss or damage and abuse, while simultaneously supporting the need for safe information exchange.

Other policies, procedures and manuals pertaining to the ISP provide additional details for its implementation. All additional documents shall be drafted and published separately.

2. SCOPE OF APPLICATION

ISP shall apply to all the CA employees and other individuals and subjects who are in any way included in business processes in accordance with the contractual or other obligations and have been granted authorized access to CA data.

Everyone stated above shall be obliged to sign the "ISP Acceptance Statement" and adhere to its provisions, all with the aim of enabling safe operation of the information system, and with the purpose of it being to maintain uninterrupted operation.

ISP shall also apply to the overall CA information structure, to include all information system resources.

3. INFORMATION SYSTEM POLICY OBJECTIVES

- Identifying grounds and responsibilities for the implementation of the Information System Policy;
- Defining methods and procedures for the implementation of security and protection of CA information system;
- Provide continuous implementation of ISP.

4. INFORMATION CONFIDENTIALITY AND PROTECTION

1) All CA employees are obliged to secure data and information that they are processing while working. Information security starts from regular filing and storage of data, to securing access and data management.

2) CA information system shall be used by its employees for official purposes only. Personal use of information system is not allowed.

3) All CA employees who are granted access to personal information of third parties must perform their duties in accordance with the "Law on Personal Data Protection" ("Official Gazette of Montenegro 79/08 and 70/09).

5. ROLES AND RESPONSIBILITIES

- CA management, Security and Standardization Group and Information Security Advisor (ISA) shall be responsible for the implementation of the information system security policy objectives;
- ISA shall prepare monthly reports on information security and provide recommendations for action;
- ISA shall coordinate activities relating to security policy, implementation and introduction of improvements. They shall be responsible for updating documentation pertaining to the security policy;
- Heads / chiefs of organizational units monitor the implementation of the information security policy in their fields of work, and they also share the policy with their employees;
- All information system users must familiarize themselves with the data and information system security rules, as well as with the procedures pertaining to the same. Security standards must be implemented and adhered to;
- All CA employees are obliged to responsibly use all information system resources assigned to them for work related purposes;
- If the employees take notice of unauthorized access to the information system, they must inform their superiors and ISA thereof.

6. INFORMATION SECURITY POLICY IMPLEMENTATION

6.1 Security Requirements

- Security regulations for equipment and process control must be in accordance with CA procedures;
- Implementation of ISP must be subject to regular control and monitoring. If it is determined that security process could be modified or improved, such modifications shall be introduced accordingly.

6.2 Provision of Physical Security

- Physical security must be provided in order to prevent unauthorized access, damage or interruptions during CIS operation;
- IT protection level must be in accordance with the value of protected assets, risks and security criteria;
- IS resources are key to the operation of the overall information system and must be secured from unauthorized access. IT equipment must be placed in secured premises with access granted only to authorized persons;
- Safety mechanisms must be implemented in order to provide physical security, i.e. prevent theft, destruction and other risks (fire, floods, damage due to power outages);
- Access of CA employees and other individuals to the IS resources must be controlled and monitored.

6.3 System Access Control

- Procedures for monitoring the granting of system access rights must be established;
- Responsibilities and procedures pertaining to security system control must be documented;

- In order to identify users and check user rights, a procedure for allocation of user passwords and right must be established, as well as a procedure for regular change of user passwords;
- System access and manner of operation by the user shall be controlled and monitored. This is of utmost importance for continuous monitoring of unauthorized system access;
- LAN access shall be controlled and monitored. During their work on the computer, users must not put the security of other computer networks or services at risk;
- Security mechanisms must include adequate approval process for remote location user access.

6.4 Personal Responsibility

- Security procedures must be presented right upon the hiring of new employees or at their transfer within the organization with the aim of mitigating risks of human errors, thefts, fraud or equipment abuse;
- IS access rights for each and every employee whose field of work within the organization changes shall be changed and modified in accordance with the new position;
- All CA employees shall familiarize themselves with the procedure for reporting security related incidents;
- Employees are not allowed to add, modify or remove software from the computers they are using;
- Employees are forbidden from using illegal software;
- IT and software equipment shall not be taken out of the CA, and its work location shall not be changed without a prior approval of the competent organizational unit;
- Prior to being given the rights to use the information system resources, all users shall be provided with adequate training.

6.5 Use of Computers and Software Applications

All CA employees are obliged to review the handbooks on the use of work stations/software and follow and adhere to the security and data protection guidelines, as well as antivirus protection.

6.6 System Development

- During the course of the development of software/applications, the development environment shall be separated from the testing and production environment;
- During software/application testing, testing environment shall be separated from the production environment;
- Standards and procedures for software development, installation and testing shall be complied with during the development process. The standards and procedures shall be defined in a way that the development system meets CA user requirements in the context of quality, security and functionality;
- Information system development, modification and upgrade shall comply with the standards. Standards must be regularly reviewed and adjusted on as needed basis;
- The system shall be protected from unauthorized modifications.

7. DOCUMENTATION

7.1 Availability of Documentation

- Procedures for the implementation of this policy are documented in other policies, handbooks and manuals. All additional documentation represents an integral part of this Information Security Policy;
- All CA employees shall familiarize themselves with the Information Security Policy, accompanying documents and the location at which the same shall be made available.

7.2 Changes

- Information Security Policy implementation is an ongoing process. The process shall be updated if there are changes involving the technology, use, procedures, laws or risks.
- Information Security Advisor shall be responsible for making changes to the Information Security Policy and respective documentation;
- Changes shall be approved by the Customs Administration management (Director).

8. MONITORING OF INFORMATION SECURITY POLICY AND PROCEDURES

8.1 Procedure Compliance and Monitoring

At regular intervals (once in 6 months), ISA shall monitor the compliance of the security implementation level with the Information Security Policy. All findings shall be documented and reported to the management.

8.2 Violation of Security Rules and Reporting of Violations

- Incidents that are not in accordance with the Information Security Policy, standards and instructions shall be treated as violations of the same;
- All employees who take notice of such cases shall immediately report the same to their supervisors or ISA;
- If necessary, ISA shall conduct an investigation, draft a report thereof and inform the management about their findings.

8.3 Sanctions in Case of Violation of Information Security Policy Rules

In case of violation of rules from the Information Security Procedure, the heads of organizational units shall initiate activities with the CA Director for sanctioning the employee in accordance with the applicable legislation.

9. TRANSITORY AND FINAL PROVISIONS

Information Security Policy shall enter into force on the date of its signing by the CA Director and publishing on CA website.

D I R E C T O R
Vladan Joković

CO : 02, a/a