COPY

REGENT SUKOHARJO
PROVINCE OF CENTRAL JAVA

SUKOHARJO REGENCY REGULATIONS
NUMBER 71 OF 2021
ABOUT
ORGANIZATION OF ENVIRONMENT FOR SECURING INFORMATION
IN THE ENVIRONMENT OF THE SUKOHARJO DISTRICT GOVERNMENT

BY THE GRACE OF GOD ALMIGHTY

REGENT SUKOHARJO,

Considering: a. that in order to secure information within the Sukoharjo Regency Government, it is necessary to administer coding based on norms, standards, procedures and criteria in accordance with the provisions of statutory regulations;

b. that based on the provisions of Article 12 paragraph (2) National Cyber and Crypto Agency Regulation Number 10 of 2019 concerning the Implementation of Encryption for Information Security in Regional Governments, states that the Governor or Regent/ Mayor, in accordance with their authority, is responsible for implementing encryption for information security;

c. that based on the considerations as intended in letters a and b, it is necessary to stipulate a Regent's Regulation concerning the Implementation of Encryption for Information Security within the Sukoharjo Regency Government;

Remember : 1. Law Number 13 of 1950 concerning the Establishment of Regency Regions within the Province of Central Java as amended by Law Number 9 of 1965 concerning the Establishment of the Batang II Level Region by amending Law No. 13 of 1950 concerning the Establishment Regency Areas within the Province of Central Java (State Gazette

1965 Number 52, Supplement to State Gazette Number 2757);

2. Law Number 23 of 2014 concerning Regional Government (State Gazette of the Republic of Indonesia of 2014 Number 244, Supplement to the State Gazette of the Republic of Indonesia Number 5587)

   as amended several times, most recently by Law Number 11 of 2020 concerning Job Creation (State Gazette of the Republic of Indonesia of 2020 Number 245, Supplement to State Gazette of the Republic of Indonesia Number 6573);

3. Presidential Regulation Number 28 of 2021 concerning the National Cyber and Crypto Agency (State Gazette of the Republic of Indonesia of 2021 Number 101);

DECIDE:

To stipulate: REGENT'S REGULATION CONCERNING THE ORGANIZATION OF COMMANDING FOR SECURING INFORMATION IN THE SUKOHARJO DISTRICT GOVERNMENT ENVIRONMENT.

PIG

GENERAL REQUIREMENTS

article 1

In this Regent's Regulation what is meant by:

1. The region is Sukoharjo Regency.
2. Regional Government is the Regent as the organizing element of Regional Government which leads the implementation of government affairs which are the authority of the autonomous region.
3. The Regent is the Regent of Sukoharjo.
4. Regional Apparatus is the supporting element of the Regent and the Regional People's Representative Council in the implementation of Government Affairs which fall under the authority of the Region.
5. The Communication and Informatics Service is the Communication and Informatics Service of Sukoharjo Regency.
6. Encryption is an activity in the field of data/information security carried out by applying crypto concepts Which, theories, art and science along with other supporting sciences in a systematic, methodological and consistent manner and related to the ethics of the coding profession.
7. Information Security is the maintenance of confidentiality, authenticity, integrity, availability and irrefutability of Information.

8. Information Security is all efforts, activities and actions to realize Information Security.

9. Electronic System is a series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit and/or disseminate electronic information.

10. Electronic Certificate is an electronic certificate containing an electronic signature and identity indicating the legal subject status of the parties in an electronic transaction issued by an electronic certification provider.

11. Information Security Services are the output of the implementation of 1 (one) or several activities for administering Government Affairs in the Encryption sector and which have beneficial value.

12. Users of Information Security Services, hereinafter referred to as Service Users, are parties who utilize Information Security Services.

13. The National Cyber and Crypto Agency, hereinafter abbreviated to BSSN, is a government agency that carries out government duties in the field of cyber security and encryption.

Section 2

This Regent's Regulation is intended as a guideline for Regional Governments in implementing policies, programs and activities for administering coding for Information Security.

Article 3

Implementation of coding to secure information in Regional Government aims to:

a. creating harmonization in implementing coding for information security between the Central Government and Regional Governments;

b. increase the commitment, effectiveness and performance of Regional Governments in implementing policies, programs and activities for implementing Encryption for Information Security; And

c. provide guidelines for Regional Governments in establishing code communication relationship patterns between Regional Apparatus.

CHAPTER II

SCOPE

Article 4

The scope of Coding Administration includes the following stages:

a. planning;

b. implementation;

c. cooperation;

d. monitoring, evaluation and reporting; And

e. funding.

CHAPTER III

PLANNING

Article 5

Regional Coding Implementation Planning integrated Regional with development planning document in the form of Regional Long Term Development Plans (RPJPD), Regional Medium Term Development Plans (RPJMD), and Regional Government Work Plans (RKPD).

CHAPTER IV

IMPLEMENTATION

Article 6

(1) Implementation of encryption for security Regional information consists of:

a. providing analysis of the need for coding for information security;

b. provision of coding administration policies for information security;

c. information management and protection; d.

management of coding resources including human resources, password materials and password communication networks as well as budget;

e. carrying out coding support operations for information security;

f. supervision and evaluation of the implementation of information security through coding in all Regional Apparatus; And

g. coordination and consultation on coding implementation for information security.

(2) Information security as intended in paragraph (1) includes physical security, logical security and administrative protection.

(3) Procedures for Providing Encryption to secure information in the Region as stated in the Attachment which is an inseparable part of this Regent's Regulation.

CHAPTER V

COOPERATION

Article 7

In administering coding, the Regional Government can collaborate with other districts/cities
and Provincial Government.

CHAPTER VI

MONITORING, EVALUATION AND REPORTING

Article 8

(1) Monitoring and evaluation is carried out on the implementation of coding for securing regional government information.

(2) The Communication and Informatics Service carries out monitoring and evaluation as intended in paragraph (1) once every 1 (one) year.

(3) The Communication and Informatics Service submits a report on the results of monitoring and evaluation as intended in paragraph (1) to the Regent.

Article 9.

Monitoring, evaluation and reporting on the implementation of Encryption for Securing Regional Government Information as intended in Article 8

carried out in accordance with the provisions of statutory regulations.

CHAPTER VII

FUNDING

Article 10

Funding for the implementation of coding for securing regional government information comes from:

a. Regional Revenue and Expenditure Budget; and/or

b. other legitimate and non-binding sources in accordance with the provisions of statutory regulations.

CHAPTER VIII

CLOSING

Article 11

This Regent's Regulation comes into force on the date of promulgation.

So that everyone is aware, this Regulation is ordered to be promulgated by placing it in the Regional Gazette of Sukoharjo Regent Regency.

Stipulated in Sukoharjo on
December 16 2021

REGENT SUKOHARJO,

signed.

ETIK SURYANI

Promulgated in Sukoharjo on
December 16 2021

REGIONAL SECRETARY
SUKOHARJO DISTRICT,

signed.

WIDODO

REGIONAL NEWS SUKOHARJO DISTRICT
YEAR 2021 NUMBER 72

The copy corresponds to the original
HEAD OF LEGAL SECTION,

signed

RETNO WIDIYANTI B, SH
NIP Level I
Arranger. 19790801 200501 2 010

ATTACHMENT
SUKOHARJO REGENCY REGULATIONS
NUMBER 71 OF 2021
ABOUT
ORGANIZATION OF JOINNINGS
FOR INFORMATION SECURITY
IN THE GOVERNMENT ENVIRONMENT
SUKOHARJO DISTRICT

PROCEDURES FOR ORGANIZING PROTECTION FOR SECURITY INFORMATION IN THE REGION

1. Providing a policy for administering coding to secure information. A policy for administering coding for securing information in Regional Government in the form of Regent Regulations, Head of Service Regulations, Guidelines, Implementation Instructions, Technical Instructions, or *Standard Operating Procedures* (SOP). These policies may include:

a. coding governance policy, consisting of:

1) information management and protection;

2) procedures for classifying the level of confidentiality of

information; 3) controlling access to information; And

4) password communication network management.

b. operational policy for password security, consisting of:

1) safeguarding the confidentiality, integrity, authenticity and non-repudiation of information and systems using electronic certificates;

2) securing devices and data processing facilities and information;

3) security of password communication networks;

4) implementation and security of video conferences;

5) implementation of counter sensing and jamming; And

6) one-stop service for sending and receiving information.

c. Encryption Resource management policy, consisting of:

1) fulfillment of HR competency and quantity; 2) controlling

access to matsan and password communication nets;

3) general maintenance and repair of the matsan;

4) provision of matsan and password communication networks; And

5) increasing awareness of information security.

d. monitoring and evaluation policies for coding operations.

2. Providing analysis of coding needs for information security.
   Activities to analyze coding implementation needs include:

   a. identification of communication relationship patterns used by Regional Government, consisting of:

      1) identify the flow of information communicated between Regional Apparatus; And

      2) identify and/or provide information and communication technology facilities and infrastructure used by the Regent.

   b. determine the results of identification and analysis of password communication relationship patterns containing connected and unconnected entities in the communication relationship pattern, as well as the duties and responsibilities of each entity for the facilities and services provided.

3. Information management and protection in Regional Government includes the following matters:

   a. facilitation of determining the level of confidentiality of classified information;

   b. management and protection of exempt public information/ classified information.

      1) management of exempt public information/classified information including creation, labeling, shipping, storage;

      2) protection of excluded public information/information Classified includes:

         a) physical protection is carried out through room access control, installation of trellises and double locks, installation of CCTV;

         b) administrative protection: implementation of administrative protection is carried out based on policies, standards and operational procedures for safeguarding excluded/classified public information;

         c) logical protection *(logical security),* namely:

            (1) *logical security* using cryptography and steganography techniques to fulfill the aspects of: confidentiality, integrity, authentication and non-repudiation; And

            (2) *logical security* that uses cryptographic and steganographic techniques must meet standards and be recommended by BSSN.

   c. management and protection of open information;

   d. implementation of a Cipher Communication Network (JKS) for information security; And

   e. application of electronic signatures and encryption to information.

4. Management of Encryption Resources consisting of:

   a. Human Resources (HR) management includes:

      1) planning the needs of human resources working in the coding sector is prepared taking into account the number and competencies required. In this planning activity, the unit that handles coding can prepare a Workload Analysis (ABK) and Sandiman Functional Position Formation and submit proposals for these needs to the Regional Personnel Agency;

      2) developing the competency of human resources who work in the coding sector, including through Sandiman Functional Training (Formation and Leveling), Cipher Technical Training, Guidance Technical/Assistance/Workshop/Seminar related to Encoding and Information Technology as well as other required fields of knowledge;

      3) submission of Encryption Security Allowance (TPP) as a form of compensation for responsibility in carrying out tasks in the field of encryption administration for password security;

      4) submission of Sandiman Functional Position Allowances for employees appointed to Sandiman Functional Positions and

      5) submit a proposal for awarding an Award in the Coding Sector for human resources working in the encoding sector who have met the requirements to the Head of BSSN.

   b. Management of Facilities and Infrastructure includes:

      1) management of Matsan (Code Material) and JKS includes:

         a) fulfillment of the needs of the matsan to be used in the implementation of external JKS by the Regional Government can be facilitated by BSSN by submitting an application to BSSN according to the results of the needs analysis;

         b) meeting the needs of matsan that will be used in the implementation of JKS in accordance with the needs analysis; And

         c) matsan storage (cipher equipment and cipher system keys) based on applicable provisions.

      2) Management of Encryption Main Support Tools (APU) includes:

         a) fulfillment of Encryption APU can be carried out independently by requesting a recommendation from BSSN or submitting an application for the use of Encryption APU to BSSN;

         b) storage of APU Encryption taking into account Security requirements include:

            (1) the APU Encryption storage location must be equipped with access controls to prevent the risk of loss, damage and manipulation; And

(2) Encoding APUs are prohibited from being used, borrowed, or taken outside the work space or office without permission from the person in charge of Matsan management.

c) Encoding APU maintenance is carried out by carrying out maintenance and repairs (if there is damage) in accordance with the authority possessed.

5. Implementation of coding support operations for security Regional Government information includes:

a. jamming carried out according to the request and used accordingly its limitations.

b. counter sensing

1) counter sensing is carried out on rooms used by Regional Government Leadership to convey classified information;

2) counter-sensing activities are carried out through physical inspection of the room by paying attention to items in the room that have the potential to become surveillance equipment ;

3) findings from counter-sensing results in the form of items suspected of being surveillance equipment *can* be consulted with BSSN;

4) the implementation of counter-sensing activities is carried out systematically periodic;

5) Regional Governments can carry out counter-sensing activities independently. If you cannot do it independently, you can submit a request for counter-sensing activities to BSSN.

c. implementation of Information System Security assessment activities

1) Information System Security assessment activities are carried out by examining whether or not there are vulnerabilities in the Information System; And

2) Regional Governments can carry out Information System Security Assessment activities independently. If you cannot do it independently, you can submit an Information System Security Assessment request to BSSN.

d. Electronic Certificate Services

1) The implementation of electronic certificate service activities can be carried out by the Regional Government if it has fulfilled the requirements and has been given authority by the Electronic Certification Center (BSrE), BSSN.

2) electronic certificate service activities carried out include:

a) registration and application for issuance, revocation and electronic certificate renewal;

b) development of applications supporting the use of certificates electronic;

c) technical guidance and outreach regarding the use of certificates electronic; And

d) monitoring and evaluating the use of electronic certificates.

3) procedures for using electronic certificates in the environment Regional Government is regulated in separate regulations.

e. The implementation of the Security Operation Center (SOC) can be carried out independently but still in collaboration with BSSN as the supervisory agency where the SOC infrastructure in the Regional Government can be centralized and connected to BSSN, so that activities will be responsive.

6. Supervision and evaluation of the implementation of information security through coding in all Regional Apparatus.

Supervision and evaluation are intended to monitor developments, identify obstacles and improve efforts in the implementation of coding for information security.

a. Supervision and evaluation of the implementation of coding by the Regional Government must be reported to the Provincial Government so that it can be followed up with an improvement plan as input for the preparation of policies, programs and activities for the implementation of coding in the following year

b. supervision and evaluation of coding administration implementation includes:

1) routine and incidental supervision and evaluation as following:

a) monitoring the use of matsan, password applications, and/or other encoding service facilities;

b) implement risk management policies for the implementation of coding in the Regional Government. This monitoring and evaluation activity is carried out by taking into account the following provisions:

(1) The Regional Government implements management policies risks determined by BSSN;

(2) Device Organizing area Encryption carries out the function of coordinating the implementation of risk management policies for the administration of Encryption; And

(3) In the event that there is a potential incident and/or the occurrence of an incident in the administration of encryption and information security, the Regional Government assists in carrying out the task of a Special Encryption Examination (special audit) or an investigation carried out by BSSN regarding an incident in the administration of encryption and information security.

2) Annual monitoring and evaluation as follows:

a) measurement of the level of utilization of Encoding services by Local government.

When measuring the level of utilization of Encryption services, it is necessary to pay attention to the following matters:

(1) the number of Regional Apparatuses that utilize the analysis the need for information security coding for implementation;

(2) the number of Regional Apparatus carrying out management and Information protection; And

(3) the number of Regional Apparatuses that utilize the operational services for Encryption support for information security.

b) self-assessment *of* the implementation of coding in the Regional Government. This monitoring and evaluation activity is carried out by taking into account the following provisions: (1) self-assessment *is* a measurement of independent coding

implementation carried out using the coding implementation measurements that have been determined by the BSSN; And

Instrument

(2) in carrying out a self-assessment , high objectivity is required in accordance with the conditions of coding implementation in the Regional Government. Therefore, valid supporting evidence is needed so that the results can be justified;

(3) *self-assessment* is carried out by human resources who are code qualified, have mastered audit techniques and have followed technical guidance on the use of

Instrument for Measuring Encryption Implementation determined by BSSN;

(4) in the event that the Communication and Information Technology Service has limited human resources, it must consult with BSSN to determine further policies;

(5) self - assessment will produce a temporary independent opinion regarding implementation

Encoding in Regional Government; And

(6) the results of the self-assessment *are* reported regularly especially for BSSN.

c) measuring the level of satisfaction of Regional Apparatus with Encryption services managed by the Regional Apparatus administering Encryption.

This monitoring and evaluation activity is carried out by taking into account the following provisions: (1) the preparation of

instruments for measuring the level of satisfaction of Regional Officials with Encryption services is carried out using a scientific approach and testing for validity and reliability is carried out. The measurement instrument is prepared according to the service object whose satisfaction will be measured; And

(2) Regional Governments can consult with BSSN regarding the use of instruments to measure the level of satisfaction of Regional Officials with Encryption services.

d) preparation of the Regional Government's Annual Encryption Implementation Report (LP2T).

This monitoring and evaluation activity is carried out by taking into account the following provisions:

(1) LP2T contains the results of the implementation of policies, programs and technical activities including the results of monitoring and evaluation activities which describe the results of the implementation of government affairs in the Encryption sector for one year; And

(2) Coordinate the preparation of materials and carry out the preparation of the LP2T.

7. Coordination and consultation on coding implementation for information security.

In the context of implementing government affairs in the coding sector, the Communications and Information Service can carry out coordination and/or consultations with BSSN, related regional apparatus and other regional governments.

REGENT SUKOHARJO,

signed.

ETIK SURYANI