COPY

REGENT SUKOHARJO
PROVINCE OF CENTRAL JAVA

SUKOHARJO REGENCY REGULATIONS
NUMBER 65 OF 2022
ABOUT

SECURITY BASED GOVERNMENT SYSTEM
ELECTRONIC

BY THE GRACE OF GOD ALMIGHTY

REGENT SUKOHARJO,

Considering: that to implement the provisions of Article 24 paragraph (4) Sukoharjo Regency Regional Regulation Number 2 of 2022 concerning Electronic-Based Government Systems, need to establish a Regent's Regulation on Security Electronic Based Government System;

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 Level II Region by amending Law No. 13 of 1950 concerning the Establishment of Regency Regions within the Province of Central Java (State Gazette of 1965 Number 52, Supplement to State Gazette Number 2757);

2. Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843) as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952);

3. Law Number 14 of 2008 concerning Openness of Public Information (State Gazette of the Republic of Indonesia of 2008 Number 61, Supplement to State Gazette of the Republic of Indonesia Number 4846);

4. Law Number 23 of 2014 concerning Regional Government (State Gazette of the Republic of Indonesia of 2014 Number 244, Supplement to 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 Republic of Indonesia 2020 Number 245, Supplement to the State Gazette of the Republic of Indonesia Number 6573);

5. Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2019 Number 185, Supplement to State Gazette of the Republic of Indonesia Number 6400);

6. Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (State Gazette of the Republic of Indonesia of 2018 Number 182);

7. Presidential Regulation Number 39 of 2019 concerning One Indonesian Data (State Gazette of the Republic of Indonesia of 2019 Number 112);

8. Presidential Regulation Number 132 of 2022 concerning National Electronic-Based Government System Architecture (State Gazette of the Republic of Indonesia of 2022 Number 233);

9. Sukoharjo Regency Regional Regulation Number 12 of 2016 concerning the Formation and Structure of Regional Apparatus (Sukoharjo Regency Regional Gazette of 2016 Number 12, Supplement to Sukoharjo Regency Regional Gazette Number 236) as amended by Sukoharjo Regency Regional Regulation Number 7 of 2022 concerning Amendments to Regulations Sukoharjo Regency Regional Number 12 of 2016 concerning the Formation and Structure of Regional Apparatus (Sukoharjo Regency Regional Gazette of 2022 Number 7, Supplement to Sukoharjo Regency Regional Gazette Number 307);

10. Sukoharjo Regency Regional Regulation Number 2 of 2022 concerning Electronic-Based Government Systems (Sukoharjo Regency Regional Gazette of 2022 Number 2, Supplement to Sukoharjo Regency Regional Gazette Number 303);

DECIDE:

To stipulate: REGENT'S REGULATION CONCERNING SECURITY OF ELECTRONIC-BASED GOVERNMENT SYSTEMS.

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. The Regional Secretary is the Regional Secretary of Sukoharjo Regency.
5. Central agencies are ministries, non-ministerial government agencies, secretariats of state agencies, non-structural agencies and other government agencies.
6. Electronic-Based Government System, hereinafter abbreviated as SPBE, is government administration that utilizes information and communication technology to provide services to SPBE Users.
7. SPBE security is integrated security control in SPBE.
8. SPBE Security Management is a series of processes to achieve effective, efficient and sustainable implementation of SPBE security, as well as supporting quality SPBE services.
9. SPBE services are outputs produced by 1 (one) or several SPBE application functions and which have useful value.
10. SPBE Application is one or a collection of computer programs and procedures designed to perform tasks or functions of the SPBE Service.
11. Intra Network is a closed network that connects network nodes within an organization.
12. Service Liaison System is an integration/connection device for exchanging SPBE Services.
13. SPBE infrastructure is all hardware, software, and facilities that are the main support for running systems, applications, data communications, data processing and storage, integration/connection devices, and other electronic devices.

14. *Application Programming Interface ,* hereinafter abbreviated as API, is a collection of commands, functions and protocols that integrate two parts of an application or different applications simultaneously.

15. Data Center is a facility used for placing electronic systems and other related components for the purposes of placement, data storage and processing, and data recovery.

CHAPTER II

SCOPE

Section 2

The scope of this Regent's Regulation includes:
a. SPBE information security management guidelines;
b. SPBE Security technical standards and procedures; And
c. funding.

CHAPTER III

MANAGEMENT GUIDELINES SPBE INFORMATION SECURITY

Article 3

SPBE information security management is implemented by the Regional Government based on SPBE information security management guidelines.

Article 4

(1) The SPBE information security management guidelines as intended in Article 3 are a reference in implementing a series of information security management processes which include:

a. scope determination; b. determination of the person in charge; c. planning; d. operations support; e. performance evaluation; and f. continuous improvement.

(2) The Regional Government communicates and documents SPBE information security management activities.

Article 5

(1) The Regent determines the scope as intended in Article 4 paragraph (1) letter a.

(2) Determination of the scope as intended in paragraph (1) is carried out by defining: a. internal issues of SPBE information security in organization; and
b. external issues of SPBE information security.

(3) Internal SPBE information security issues in the organization as referred to in paragraph (2) letter a are defined based on the organization's priority areas regarding the implementation of SPBE information security.

(4) The organization's priority areas for the implementation of SPBE information security as referred to in paragraph (3) include at least: a. SPBE data and information; b. SPBE application; c. SPBE Infrastructure assets; and D. SPBE's existing information security policy owned.

(5) SPBE external information security issues as referred to in paragraph (2) letter b are defined in accordance with the provisions of statutory regulations.

Article 6

(1) The determination of the person in charge as intended in Article 4 paragraph (1) letter b is carried out by the Regent.

(2) The person in charge as referred to in paragraph (1) is held by the Regional Secretary as the SPBE coordinator.

Article 7

(1) In carrying out duties as person in charge of SPBE Security, the SPBE coordinator as intended in Article 6 paragraph (2) determines the technical implementer of SPBE Security.

(2) SPBE Security technical implementer as follows referred to in paragraph (1) consists of:

a. Pratama high leadership officials who carry out duties and functions in the fields of technology, information and communication security in the Regional Government; And

b. high management officials or administrator officials who supervise, build, maintain, and/or develop the SPBE Application.

Article 8

(1) Pratama high leadership officials who carry out duties and functions in the field of technology, information and communication security as intended in Article 7 paragraph (2) letter a have the following duties: a. ensure implementation of technical standards and procedures SPBE Security; b. formulate, coordinate and implement the SPBE Security work program and budget; and c. report the implementation of SPBE information security management and the implementation of technical standards and SPBE Security procedures to the Regional Government SPBE coordinator.

(2) High management officials or administrator officials who supervise, build, maintain and/or develop the SPBE Application as intended in Article 7 paragraph (2) letter b have the following duties: a. implement technical standards and application security procedures in each work unit; b. ensure that all construction or development of SPBE Applications and Infrastructure carried out by third parties meets the established technical standards and SPBE Security procedures; c. ensure the continuity of SPBE business processes;

And

d. coordinate with high ranking pratama officials who carry out duties and functions in the fields of technology security, information and communication related to the formulation of SPBE Security work programs and budgets.

Article 9

(1) Planning as intended in Article 4 paragraph (1) letter c is carried out by the SPBE Security technical implementer.

(2) Planning as intended in paragraph (1) done by formulating:
a. SPBE Security work program which is structured based on SPBE Security risk categories; And
b. SPBE Security work program realization targets.

(3) The SPBE Security work program as referred to in paragraph (2) letter a includes at least: a. SPBE Security awareness education; b. SPBE Security vulnerability assessment; c. increased SPBE Security; d. SPBE Security incident handling; and e. SPBE Security audit.

(4) The SPBE Security risk category as intended in paragraph (2) letter a is determined in accordance with the provisions of statutory regulations.
(5) The target for the realization of the SPBE Security work program as intended in paragraph (2) letter b is determined based on the needs of the Regional Government.

Article 10

SPBE Security awareness education as intended in Article 9 paragraph (3) letter a is carried out at least through the following activities:

a. socialization; And
b. training.

Article 11

The SPBE Security vulnerability assessment as intended in Article 9 paragraph (3) letter b is carried out at least through:

a. inventory all SPBE assets including data and information, applications, and infrastructure;
b. identify vulnerabilities and threats to SPBE assets; And

c. measure the level of SPBE Security risk.

Article 12

(1) SPBE Security Improvement as intended in Article 9 paragraph (3) letter c is carried out based on the results of the SPBE Security vulnerability assessment as intended in Article 11.

(2) SPBE Security Improvement is implemented at least through:

a. implement technical standards and SPBE Security procedures; And
b. testing the security functions of the SPBE Application and SPBE Infrastructure.

Article 13

Handling of SPBE Security incidents as intended in Article 9 paragraph (3) letter d is carried out at least through:

a. identify the source of the attack;
b. analyze information relating to subsequent incidents;

c. prioritize incident handling based on the level of impact that occurs;
d. documenting evidence of incidents that occurred; And
e. mitigate or reduce the impact of Security risks SPBE.

Article 14

The SPBE Security Audit as intended in Article 9 paragraph (3) letter e is carried out in accordance with the provisions of statutory regulations.

Article 15

(1) Operation support as intended in Article 4 paragraph (1) letter d is carried out by the SPBE coordinator.

(2) Operation support as intended in paragraph (1) is carried out by increasing capacity for: a. SPBE Security human resources; and b. SPBE
Security budget.

(3) SPBE Security human resources as referred to in paragraph (2) letter a must have at least the following competencies:

a. security of technological infrastructure, information and communication; And
b. application security.

(4) To fulfill the competency as intended in paragraph (3), the Regional Government must at least carry out the following activities: a. training and/or competency
certification for technology infrastructure security, information and communications and application security; And

b. technical guidance regarding Security standards SPBE.

(5) The SPBE Security Budget as referred to in paragraph (2) letter b is prepared based on plans that have been determined in accordance with the provisions of statutory regulations.

Article 16

(1) Performance evaluation as intended in Article 4 paragraph (1) letter e is carried out by the SPBE coordinator.
(2) Performance evaluation as intended in paragraph (1) is carried out on the implementation of SPBE Security.
(3) Performance evaluation as intended in paragraph (2) is carried out by: a. identify process
areas that have a high risk to the successful implementation of SPBE Security;

b. establish performance indicators in each area process;
c. formulate the implementation of SPBE Security by quantitatively measuring the expected performance;

d. analyze the effectiveness of SPBE Security implementation; and
e. support
and realize the audit program
SPBE Security.

(4) Performance evaluation as intended in paragraph (1) is carried out at least 1 (one) time in 1 (one) year.

Article 17

(1) Continuous improvement as referred to in
Article 4 paragraph (1) letter f is carried out by technical implementers
SPBE Security.

(2) Continuous improvement as referred to in paragraph (1) is a follow-up to the results of the performance evaluation.

(3) Continuous improvement as intended in paragraph (1) is carried out by:
a. overcome problems in the implementation of SPBE Security; And

b. improve SPBE Security implementation
periodic.

CHAPTER IV
TECHNICAL STANDARDS AND
SPBE SECURITY PROCEDURES

Part One
General

Article 18

(1) Regional Government must implement Security
SPBE.

(2) The implementation of SPBE Security as intended in paragraph (1) must comply with SPBE Security technical standards and procedures.

Article 19

SPBE technical standards and Security procedures as follows
as intended in Article 18 paragraph (2) is applied to:
a. data and information security; b. SPBE
Application security; c. security of
the Service Connecting System;
d. Intra Network security; And
e. data center security.

The second part
Data and Information Security

Article 20

The technical standards for data and information security as intended in Article 19 letter a consist of fulfilling the following aspects:

a. confidentiality;
b. authenticity;
c. wholeness;
d. irrefutability; And
e. availability.

Article 21

Fulfillment of the confidentiality aspect as intended in Article 20 letter a is carried out using the following procedures:
a. establish information classification;
b. implement encryption with a cryptographic system; And
c. implement restrictions on access to data and information in accordance with established authorities and policies.

Article 22

The fulfillment of the authenticity aspect as intended in Article 20 letter b is carried out using the procedure:
a. provide verification mechanisms;
b. provide validation mechanisms; And
c. implementing a *hash function system.*

Article 23

Fulfillment of the integrity aspect as intended in Article 20 letter c is carried out using the following procedures:
a. implement modification detection; and b. apply a certified electronic signature.

Article 24

The fulfillment of the non-denial aspect as intended in Article 20 letter d is carried out using the procedure:

a. implement certified electronic signatures; and b. guarantee by the electronic certification provider via electronic certificate.

Article 25

Fulfillment of the availability aspect as intended in Article 20 letter e is carried out using the procedure:
a. implement a regular backup system;
b. make plans to ensure data and information can always be accessed; And
c. implement a recovery system.

Part Three
SPBE Application Security

Article 26

(1) Technical standards and security procedures for the SPBE Application as intended in Article 19 letter b are applied to: a. web-based applications;
and b. mobile based application.

(2) The web-based application as referred to in paragraph (1) letter a is an application that is accessed via a browser when connected to an internet or intranet connection.

(3) Mobile-based applications as referred to in paragraph (1) letter b are applications that can be operated on mobile devices and have an operating system that supports standalone software.

(4) The SPBE application as intended in paragraph (1) must undergo security testing every certain period which is carried out by: a. identify minimum security requirements
that have not yet been implemented;

b. ensure that the application programming coding created does not have vulnerabilities;
c. perform automatic scanning and/or system penetration testing;
d. identify vulnerabilities and manage threats early in the SPBE Application development cycle; And

e. analyze vulnerabilities.

Article 27

The technical standards for web-based application security as intended in Article 26 paragraph (1) letter a consist of fulfilling the functions of:

a. authentication;
b. session management;
c. access control requirements;
d. input validation;
e. cryptography on static verification;
f. error handling and logging;

g. data protection;
h. communications security;
i. control of malicious code;
j. business logic;
k. files;
l. API and web service security; And
m. configuration security.

Article 28

(1) Fulfillment of the authentication function as intended in Article 27 letter a is carried out using the following procedures: a. using password management for the authentication process; b. implement password verification on the server side; c. set the number of characters, combination of character types, and validity period of the password;

d. setting the maximum number of errors in password entry;

e. set up a password recovery mechanism;
f. maintain the confidentiality of saved passwords through cryptographic mechanisms; And
g. uses a secured communication path for the authentication process.

(2) The fulfillment of the session management function as intended in Article 26 letter b is carried out using the following procedures: a. uses a session handler for the process session management;
b. using session handlers provided by the application framework; c. regulates the generation and randomness of session tokens generated by the session controller; d. set the conditions and timeout period for the session; e. validation and inclusion of session ID;
f. protection of the location and delivery of tokens for authenticated sessions; And
g. duplication protection and user consent mechanisms.

(3) The fulfillment of the access control requirements as intended in Article 26 letter c is carried out using the following procedures: a. assign user authorization to limit access control;

b. set warnings against the danger of automatic attacks in the event of concurrent access or continuous access to functions;
c. setting up the interface on the administrator side; And
d. set verification of token correctness when accessing excluded data and information.

(4) Fulfillment of the input validation function as intended in Article 27 letter d is carried out using the procedure:

a. implement input validation functions on the server side;
b. implement an input rejection mechanism if a validation error occurs;
c. ensure the application *runtime environment* is not vulnerable to input validation attacks; d. perform positive validation on all input;
e. filter untrusted data;
f. using dynamic code features; g. protect access containing script content; and h. protects against base injection attacks

data.

(5) Fulfillment of the cryptographic function in static verification as intended in Article 27 letter e is carried out using the procedure:
a. use cryptographic algorithms, cryptographic modules, cryptographic protocols and cryptographic keys in accordance with statutory provisions;

b. authenticate encrypted data;
c. implement cryptographic key management; And
d. create random numbers using a cryptographic random number generator.

(6) The function of handling errors and recording logs as intended in Article 27 letter f is fulfilled using the procedure:

a. set the content of the message displayed when there is an error;
b. use error handling methods to prevent predictable and unexpected errors and handle all unhandled exceptions;

c. do not include excluded information in log recording;

d. regulate the scope of logs recorded to support investigation efforts when an incident occurs;

e. set up protection of application logs from unauthorized access and modification;
f. encrypt stored data to prevent log injection; g. synchronize time sources according to the correct time zone and time.

(7) Fulfillment of the data protection function as intended in Article 27 letter g is carried out using the procedure:

a. carry out identification and storage of copies excluded information;
b. protect against unauthorized access to excluded information temporarily stored in the application;

c. perform exchanges, deletions, and audits excluded information;
d. determine the number of parameters;
e. ensure data is stored securely;
f. define methods for deleting and exporting data according to user requests; And
g. clearing memory once it is not needed.

(8) Fulfillment of the communication security function as intended in Article 27 letter h is carried out using the following procedures:

a. use encrypted communications; b. set up secure incoming and outgoing connections and encrypted from the user side;
c. regulate the types of algorithms used and their testing tools; And
d. regulate the activation and configuration of electronic certificates issued by electronic certification providers.

(9) The fulfillment of the dangerous code control function as intended in Article 27 letter i is carried out using the procedure:

a. using code analysis in malicious code control;

b. ensure the application source code and libraries do not contains malicious code and other undesirable functionality;

c. set permissions regarding related features or sensors privacy;
d. regulate integrity protection; And
e. set the update feature mechanism.

(10) The fulfillment of the business logic function as intended in Article 27 letter j is carried out using the procedure:

a. processing business logic flows in a realistic sequence of steps and timing;
b. ensure business logic has constraints and validation;
c. monitoring unusual activity;
d. assists in anti-automation control; And
e. provides alerts when automated attacks or unusual activity occurs.

(11) Fulfillment of the file function as intended in Article 27 letter k is carried out using the procedure:
a. set the number of files for each user and upload file size quotas;
b. validate files according to content type which are expected;
c. protect input metadata and file metadata;
d. perform scanning of files obtained from untrusted sources; and e. configure the server to download files according to the specified extension.

(12) Fulfillment of API and web service security functions as intended in Article 27 letter l is carried out using the following procedures:
a. configure web services;

b. verify *the uniform resource identifier* API does not display information that could potentially be a security hole;

c. make authorization decisions;
d. displays the RESTful *hypertext transfer protocol* method if the user input is declared valid;
e. using schema validation and prior verification accept input;
f. using service-based protection methods web; And
g. implement anti-automation controls.

(13) Fulfillment of the configuration security function as intended in Article 27 letter m is carried out by the procedure:

a. configure the server according to the recommendations of the application server and application framework used;

b. document, copy configuration and all dependencies;

c. remove unnecessary features, documentation, samples, and configuration;
d. validate asset integrity if application assets are accessed externally; and e. using application responses and content safe.

Article 29

The technical standards for mobile-based application security as intended in Article 26 paragraph (1) letter b consist of fulfilling the functions of:
a. data storage and privacy requirements;
b. cryptography;
c. authentication and session management;
d. network communications;
e. platform interactions ;
f. code quality and *build settings;* And
g. resilience.

Article 30

(1) Fulfillment of the data storage function and privacy requirements as intended in Article 29 letter a is carried out using the procedure:

a. store all excluded data and information only in the system's credential storage facility;

b. limit the exchange of excluded data and information with *third parties;* c. disabling *keyboard cache* when entering excluded data and information; d. protect excluded information during *inter process communication;* and e. protects excluded data and information entered through the user interface.

(2) The fulfillment of the cryptographic function as intended in Article 29 letter b is carried out using the following procedures: a. avoid using symmetric cryptography with *hardcoded keys;* b. implements cryptographic methods has been tested according to requirements; c. avoid using obsolete cryptographic protocols or cryptographic algorithms; d. avoid using the same cryptographic key; and e. uses a random key generator meets the key randomness criteria.

(3) Fulfillment of the authentication and session management functions as intended in Article 29 letter c is carried out using the following procedures: a. implement authentication on *remote endpoints* to applications that provide user access to remote services;

b. using a random *session identifier* without the need to send user credentials when using *stateful* session management;

c. ensuring the server provides tokens that have been signed using a secure algorithm when using token-based stateless authentication;

d. ensuring remote endpoints disconnect existing sessions when users log out; e. apply password settings on the remote endpoints;
f. Limit the number of remote login attempts endpoints;
g. determine the session validity period and token expiration period on the remote endpoint; And
h. perform authorization on remote endpoints.

(4) Fulfillment of the network communication function as intended in Article 29 letter d is carried out using the following procedures:
a. implement secure socket layer or transport layer security that is not obsolete consistently; And
b. verify remote endpoint certificates.

(5) Fulfillment of the platform interaction function as intended in Article 29 letter e is carried out using the following procedures:
a. ensure applications only request access to required resources;
b. validate all input from external sources and users; c. avoid sending sensitive functionality through custom uniform resource locator schemes and inter process communication facilities;

d. avoid using JavaScript in WebView; e. using the hypertext transfer protocol secure on WebView; And
f. implements the use of secure API serialization.

(6) Fulfillment of code quality functions and build settings as intended in Article 29 letter f is carried out using the following procedures:

a. sign the application with that certificate valid;
b. ensure the application is in release mode; c. removed debugging symbols from native binary; d. removed debugging code and developer help code;

e. Identify weaknesses in all third components parties;
f. determine error handling mechanisms;
g. manage memory securely; And
h. enable available security features.

(7) The fulfillment of the resilience function as intended in Article 29 letter g is carried out using the procedure:

a. prevent applications from running on devices to which unauthorized modifications have been made;
b. detects and responds to *the debugger;*
c. prevents *executable files* from making changes on device resources;
d. detect and respond to the presence of *reverse engineering devices;*
e. prevent applications from running in the emulator; f. detect code and data changes in space memory;
g. implement *device binding* functions by using unique *properties* on the device;
h. protect all *files* and *libraries* in the application; And
i. apply the *obfuscation method.*

Part Four
Service Connecting System Security

Article 31

The security technical standards for the Service Connecting System as referred to in Article 19 letter c consist of fulfilling the functions of:

a. data and information interoperability security;
b. integration system control;
c. integrator device control;
d. API and web service security ; And
e. data migration security.

Article 32

(1) Fulfillment of data and information interoperability security functions as intended in Article 31 letter a is carried out with the procedure:

a. implement a certified electronic signature system to secure documents and electronic mail;
b. implement a data encryption system;
c. ensure data and information can always be accessed according to authority; And
d. apply a *hash function* system to *files.*

(2) Fulfillment of the integration system control function as intended in Article 31 letter b is carried out using the following procedures:
a. apply the latest version of *the secure socket layer protocol* or *transport layer security protocol* in data and information transmission sessions;

b. implementing internet *protocol security* to secure data transmission in *transmission control protocol/ internet protocol based networks;*

c. implementing an anti- *distributed denial of service system;*
d. implement authentication to verify external identity between connected SPBE Services; e. implement session security management;

f. apply user access restrictions based on predetermined authorization;
g. implement input validation;
h. applying cryptography to static verification;
i. implementing electronic certificates in *web authentication;*

j. implementing error handling and logging ;
k. implement data protection and communication lines;
l. apply a virus detector to check some *file contents;*

m. establish a service level agreement with a standard of at least 95% (ninety five percent); And

n. ensure the integration system does not have vulnerabilities that could potentially become hackers' loopholes.

(3) Fulfillment of the control function of integrator equipment as intended in Article 31 letter c is carried out using the procedure:

a. use operating systems and software with the latest *security patches ;*
b. use the latest anti-virus and *anti-spyware ;*
c. enable security features on web browsers;
d. implement *firewalls* and *host-based intrusion detection systems;*
e. prevent the installation of software that has not been installed verified;
f. prevent access to unauthorized sites; and g. activate the *recovery* and *restore* system on the *integrator device.*

(4) Fulfillment of API and *web service* security functions as intended in Article 31 letter d is carried out using the following procedures: a. implementing *a secure socket layer protocol* or *transport layer security protocol* between the sender and recipient of the API;

b. implementing the latest version *of the open authorization protocol* to bridge interactions between *resource owners, resource servers* and/or *third parties;*

c. displays the RESTful hypertext transfer protocol method if the user input is declared valid;
d. protect RESTful web services that use cookies from cross-site request forgery; And

e. validate incoming parameters by the API receiver to ensure the data received is valid and does not cause damage.

(5) Fulfillment of the data migration security function as intended in Article 31 letter e is carried out using the following procedures: a. ensure data migration is carried out in stages and programmed by the system;
b. ensure applications that use the old database system are maintained until the new database support system can run or function normally;

c. document the format of the legacy database system in detail;
d. back up all data stored on the system before migrating data;

e. apply cryptographic techniques to the data storage and retrieval process; and f. perform data validation during the data migration process finished.

Part Five
Intra Network Security

Article 33

(1) Intra Network Security technical standards as intended in Article 19 letter d are applied to Local government.
(2) Intra Network security technical standards as referred to in paragraph (1) consist of fulfilling: a. Intra Network security administration aspects;
b. access control and authentication;
c. Intra Network security device and application requirements;

d. gateway security controls;
e. access point security control on wireless networks; And

f. Control access point configuration on the network wireless.

Article 34

(1) Fulfillment of the security administration aspects of the Intra Network as intended in Article 33 paragraph (2) letter a is carried out using the following procedures: a. compose and evaluate Intra Network architecture documents;

b. identify all network infrastructure assets;
c. prepare and establish standard operational procedures related to maintaining Intra Network security; And

d. create periodic network security monitoring reports.

(2) Fulfillment of access control and authentication as intended in Article 33 paragraph (2) letter b carried out with the procedure:
a. placing network infrastructure devices that provide Intra Network services in separate zones;

b. use authentication to access the Intra Network;

c. implement access restrictions in the Network Intra;
d. disabling or limiting *protocols, ports,* and unused services;
e. implement link filtering and block access to malicious sites;

f. implement *honeypot* function to analyze security gaps based on attack type;
g. implementing *virtual private networks* and activate the encryption function on the communication line used;
h. authorizes only the administrator to install software and/or change system configuration in the Intra Network;

i. implementing *secure endpoints;*
j. block unknown services; k. apply the latest version of *secure socket layer* or *transport layer security* on the Intra Network access point; And

l. implementing an intermediary server when *the client* accesses the database server for maintenance purposes.

(3) Fulfillment of the requirements for Intra Network security devices and applications as intended in Article 33 paragraph (2) letter c is carried out using the procedure:
a. using *security information and event management* tools for *network logging* and monitoring;

b. implement an early vulnerability detection system network device security;
c. using firewall devices;

d. using *intrusion detection systems* and *intrusion prevention systems;*
e. implementing an encrypted virtual private network for limited remote access use;
f. implement *patching update* controls on Intra Network infrastructure and computer systems;
g. using a *web application firewall device;*
h. using load balancer devices to maintain the availability of access to networks and applications;

i. updating hardware and software security technologies to minimize hacker gaps;

j. downloading software via *an enterprise software distribution system;* And
k. apply electronic certificates.

(4) Fulfillment of *gateway* security controls as intended in Article 33 paragraph (2) letter d is carried out using the procedure:

a. apply *content filtering;*
b. implement *inspection packet filtering* to check incoming *packets* on the Intra Network;
c. implement security controls on access features remote *gateway device;*
d. ensure that *gateway* devices that connect intra-networks are not connected directly to public networks;

e. carry out *gateway traffic* management ; And
f. ensure *the port* is not opened by *default.*

(5) Fulfillment of *access point* security controls on wireless networks as intended in Article 33 paragraph (2) letter e is carried out using the procedure:
a. implement the latest wireless *access point* security protocols and encryption technology;
b. apply media *access control* to *the address filtering;*
c. implement *a dedicated service set identifier;*
d. implementing radio transmission range restrictions and network users;
e. implement restrictions regarding the addition of unauthorized installed wireless devices;
f. implement *vulnerability* management periodically and continuously; And
g. perform *firmware patching* regularly.

(6) Fulfillment of *access point* configuration control on the wireless network as intended in Article 33 paragraph (2) letter f is carried out using the procedure: a. use strong passwords;

b. using *authentication authorization* and *accounting* model protocols on network infrastructure devices for *user management* or *access point administrator authentication;*

c. ensure remote configuration access features can only be used in emergency situations by implementing security controls; d. isolating or segmenting wireless local area networks; and e. disable wireless interfaces, services, and unused applications.

Part Six
Data Center Security

Article 35

Data Center security technical standards as referred to in Article 19 letter e consist of fulfilling:
a. Physical security and Center management requirements Data; And
b. device connection requirements to the Data Center.

Article 36

Device connection to the Data Center with the procedure:
a. ensure the security of devices connected to the Data Center infrastructure;
b. cut off physical or logical access from unauthorized devices;

c. ensure that administrator level access to *servers* and main network devices cannot be done remotely ;

d. ensure that only authorized personnel are allowed to use computers in the Data Center area;
e. carry out regular backups of information and software in the Data Center;
f. ensure Data Center computer equipment is free from viruses and *malware;*
g. restricting access to the use of *removables* media in the Data Center area;
h. ensure that the activation of the *universal serial bus port* configuration has received permission from authorized personnel; i. ensure that every device that will be connected to the Data Center infrastructure uses *internet protocol* specified *address* and *hostname ;* And
j. implementing an intermediary *server* when *the client* accesses *the database server* for maintenance purposes.

CHAPTER V

FUNDING

Article 37

All funding for the implementation of SPBE Security is charged to the Regional Revenue and Expenditure Budget.

CHAPTER VI

CLOSING

Article 38

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 Regency.

Set in Sukoharjo
on December 28, 2022
REGENT SUKOHARJO,

signed.

ETIK SURYANI

Promulgated in Sukoharjo
on December 28, 2022

REGIONAL SECRETARY
SUKOHARJO DISTRICT,

signed.

WIDODO

REGIONAL NEWS SUKOHARJO DISTRICT
YEAR 2022 NUMBER 65

The copy corresponds to the original
HEAD OF LEGAL SECTION,

signed.

TEGUH PRAMONO, SH, MH
Level I Supervisor
NIP. 19710429 199803 1 003