



REPUBLIC OF THE PHILIPPINES
COMMISSION ON ELECTIONS
Intramuros, Manila

COMMISSION ON ELECTIONS
ITD - ADMIN
RECEIVED
TEL 11 2024
BY: Chen TIME: 6:37 AM
REF: 11-121124-A022

IN RE: POLICY AND
PROCEDURES ON SECURE
ELECTRONIC
TRANSMISSION SERVICES
(SETS) 2025 DATA CENTERS
OPERATIONS FOR THE
CONDUCT OF THE MAY 12,
2025 NATIONAL AND
LOCAL ELECTIONS AND
BARMM PARLIAMENTARY
ELECTION

X-----X

GARCIA, George Erwin M.
INTING, Socorro B.
CASQUEJO, Marlon S.
FEROLINO, Aimee P.
BULAY, Rey E.
MACEDA, JR., Ernesto Ferdinand P.
CELIS, Nelson J.

Chairman
Commissioner
Commissioner
Commissioner
Commissioner
Commissioner
Commissioner

PROMULGATED: November 20, 2024

RESOLUTION NO. 11080

WHEREAS, for the 12 May 2025 National and Local Elections (NLE) and BARMM Parliamentary Elections (BPE), the COMELEC will implement the Full Automation System with Transparency Audit/Count (FASTrAC) to align with the MakaBAGOng Halalan para sa MakaBAGOng Pilipino together with the Secure Electronic Transmission Services (SETS) that will employ the "send-to-all" parameters;

WHEREAS, four (4) Data Centers in separate locations will also be put in place to individually house the *Transparency Servers*, the *Backup Server*, the *Central Server*, and the *Mirror Server*;

WHEREAS, there is a need to prescribe the policy, guidelines, and protocol for the operations of the SETS 2025 Data Centers in relation to the 2025 NLE & BPE, which includes the minimum requirements for securing, monitoring, maintaining, protecting, and decommissioning the same;

WHEREAS, this Policy shall apply to SETS 2025 Data Centers, including all authorized persons from COMELEC, FASTrAC, and SETS 2025 providers who will be granted access to the data center, for the duration indicated in the access pass. This will also apply to all guests who will be allowed access to the Data Center for visitation and observation purposes;

NOW, THEREFORE, by virtue of the powers vested in it by the Constitution, the Omnibus Election Code, Republic Act No. 9369 and other election laws, the Commission En Banc RESOLVED, as it hereby RESOLVES, to PROMULGATE the following policy and procedures:

SECTION 1. Definitions. – As used in this Resolution:

- a. Backup Server – refers to the server which is the redundancy and the high availability measure for the Central Server;
- b. CAC – refers to the COMELEC Advisory Council;
- c. Central Server – refers to the server that will receive the electronically transmitted precinct results from all Automated Counting Machines (ACMs) and Consolidation/Canvassing System (CCS) results. This server will be the source of the website publications of election results for use by the general public;
- d. ICE – refers to the International Certification Entity
- e. JCOC – refers to the Joint Congressional Oversight Committee
- f. Media Server – refers to the server which runs the File Transfer Manager that provides copy of the Election Results to the media organization and accredited political parties;
- g. Mirror Server – refers to the server that is a redundancy measure for the Central Server, which will be housed at the Department of Information and Communications (DICT) data center facility.
- h. TEC – refers to the Technical Evaluation Committee
- i. Transparency Servers – refers to the group of servers for the Dominant Majority and Minority, the Accredited Citizens Arm 1 and 2, and the Media and which will receive the electronically transmitted precinct results from all ACMs.

SECTION 2. Responsibilities

- a. Overall responsibility for all activities done in the Data Centers shall reside with the SETS 2025 Project Director, who shall report and coordinate to the Project Management Office (PMO) Project Director;
- b. The SETS 2025 Unit of the PMO Field Operations Group shall be responsible for the monitoring of the implementation of all technological aspects of this Policy;
- c. The physical aspect of securing the Data Centers shall jointly reside with the SETS 2025 solution provider and the Administrative Services Department (ASD) under the direct supervision of the COMELEC Security Officer;
- d. More specifically, COMELEC and the *SETS 2025 provider* shall be responsible for the following:

1. COMELEC, through its SETS 2025 Team personnel in the Data Centers, shall be responsible for the following:
 - 1.1 Physical security and physical access to the Data Centers, including:
 - 1.1.1 Maintaining list of authorized personnel to enter the Data Centers;
 - 1.1.2 Allowing authorized personnel only to enter Data Centers;
 - 1.1.3 Review and maintaining list of authorized and identified user accounts, if applicable;
 - 1.1.4 Data security and data access using identified applications only;
 - 1.1.5 Creating and maintaining all user accounts; and
 - 1.1.6 Operating Data Center applications using authorized and identified user accounts based on specified user roles and privileges.
 - 1.2 Documentation of all activities in the Data Centers
2. *iONE-Ardent Joint Venture*, as Solutions Provider, in constant coordination with COMELEC, shall be responsible for:
 - 2.1 Physical and logical setting up of the Data Centers;
 - 2.1.1 Configuring the servers in the Data Centers according to the requirements of COMELEC as defined in the SETS 2025 Terms of Reference.
 - 2.2 Creating and granting the initial *Admin* user account for COMELEC;
 - 2.3 Perform technical support as deemed necessary; and
 - 2.4 Provide for solution and services necessary to make the SETS 2025 Datacenter fully operational for the FASTrAC and for the COMELEC accredited media entity.

SECTION 3. Guidelines and Protocol

a. Physical Access to the Data Centers

1. Only authorized personnel shall be allowed access to the Data Center.
 - 1.1. The authorization shall be formally issued and written for documentation and audit purposes;
 - 1.2. The authorization shall be issued by the Commission *En Banc*;
 - 1.3. The authorization shall indicate the reason and duration of the issuance of such authorization;
 - 1.4. A copy of all authorizations shall be provided to the guards on duty for reference purposes; and

- 1.5. A complete and updated list of authorized personnel shall be maintained by the guards on duty and shall be posted at the entrance of the Data Center for information purposes.
2. All personnel who will be assigned to the SETS 2025 Data Centers shall be formally designated by the Commission *En Banc*.
3. All authorized personnel shall be issued with an ID card to serve as access pass to the Data Centers by the PMO.
 - 3.1. The ID card shall bear the name and picture of the concerned authorized personnel;
 - 3.2. The ID card shall be signed by the PMO Project Director;
 - 3.3. The ID card shall always be worn before entering and while inside the Data Centers; and
 - 3.4. The ID card shall indicate the duration of access allowed for each authorized personnel accordingly.
4. Temporarily authorized persons, such as for official visit or site inspection purposes, shall be issued with Temporary Passes for the purpose.
 - 4.1. A copy of the authorization shall be provided to the guards on duty before entry for record purposes;
 - 4.2. The visit to the Data Center by the temporarily authorized persons shall be properly recorded in a Visitors Log for the purpose:
 - 4.2.1 The name and signature of a temporarily authorized person, date, and time of entry and exit from the Data Center shall be provided in the Log; and
 - 4.2.2 The SETS 2025 Team Unit Head, the PMO Field Operations Group Head, or the PMO Project Director shall accompany the temporarily authorized person from entry to and exit from the Data Center.
5. The PMO Project Director shall prescribe the necessary forms and other related documents for the purpose.
 - 5.1 For proper information and monitoring purposes, all approved forms and documents to be used in the Data Center shall be properly communicated and disseminated to all authorized personnel who will be assigned to the same; and
 - 5.2 All documentation shall be maintained by the PMO 2025 NLE.

b. Code of Conduct

1. Entry and exit to the Data Center shall be properly recorded;

2. All authorized personnel shall not be allowed to bring in any equipment, including recording and mobile devices, that has not been authorized for use inside the Data Center by the PMO Project Director or SETS 2025 Project Director;
3. All authorized personnel shall observe professional behavior while inside the Data Center:
 - 3.1 All activities by authorized personnel inside the Data Center shall be bound by the duties and responsibilities that shall be delegated to the same by COMELEC through the Commission *En Banc*;
 - 3.2 All system access rights and privileges by each authorized personnel shall be informed to all authorized personnel for check and balance purposes:
 - 3.2.1 A written copy of the same shall always be available to all authorized personnel for ready reference purposes;
 - 3.2.2 Any activity that has not been explicitly stated as authorized activity shall be formally informed to the Commission *En Banc* by the SETS 2025 Project Director for appropriate action. No action shall be taken unless there is an explicit formal instruction of the Commission *En Banc* on the appropriate action to be taken; and
 - 3.2.3 All activities by authorized personnel inside and outside of the Data Center shall be subject to the provisions indicated in the Non-Disclosure Agreement (NDA) between the same and COMELEC.
 - 3.3 Food and drinks are not allowed in the Server Room;
 - 3.4 No Internet connection shall be allowed inside the Server Room, except for those that are explicitly stated as necessary for its operation; and
 - 3.5 All activities in the Data Centers shall be monitored and recorded using CCTV.
 - 3.5.1 All CCTV footages shall be recorded with redundancy and shall be stored until upon completion of all transmission and upon the authorization of the PMO 2025 NLE & BPE Director to decommission the Data Centers.

4. Data Center Access Levels

4.1 Level 0 Access: VIP Access

- 4.1.1 This access level is provided to the Chairman and the Commissioners, the PMO Project Director, the SETS 2025 Project Director, and the PMO Group Heads;
- 4.1.2 Subject to the approval of the Commission *En Banc*, this access level shall also be provided to the JCOC Members and

representatives, CAC Members and authorized representatives, the TEC Members and authorized representatives, and ICE representatives.

- 4.1.2.1 For purposes of the TEC Certification, all activities by the TEC and the ICE shall be coordinated with the SETS 2025 Project Director and shall be performed in the presence of Level II Access personnel.
- 4.1.3 Their presence in the Data Centers shall be logged by the guards on duty in the Visitors Log;
- 4.1.4 People with VIP access shall not be subjected to frisking by the guards on duty;
- 4.1.5 Other indicated restrictions shall also apply to people with this access level; and
- 4.1.6 These persons are still subject to the policy defined by the Data Center Facilities Provider.

4.2 Level I Access: Visitor

- 4.2.1 This access level is provided to non-SETS 2025 Team personnel, including visitors who are temporarily authorized to enter the Data Centers;
- 4.2.2 People with Level I access shall only be allowed physical access into the Data Center and shall always be accompanied by the above-named authorities; and
- 4.2.3 This access level shall also be provided to political party representatives, subject to the prior approval by the Commission *En Banc*.

4.3 Level II Access: Operational Access

- 4.3.1 This access level is provided to SETS 2025 and Solutions Provider personnel;
- 4.3.2 Personnel with Level II access shall be allowed physical and logical access to the Data Center, its servers and applications, including Data Center documentation subject to the responsibilities assigned to each; and
- 4.3.3 All responsibilities and ensuing system access rights and privileges for each Level Access II personnel shall be documented.

4.4 Level III Access: Media Site Access

- 4.4.1 This access shall be provided to authorized personnel of the accredited political parties, citizens arm, and media at the Media Site Monitoring Room;
- 4.4.2 This access level shall be complemented by the signing of a Confidentiality Agreement by the authorized personnel for his/her represented organization/group;
- 4.4.3 This access shall be provided to a maximum of two (2) authorized representatives at any given time;
- 4.4.4 The concerned organization shall be assigned a unique username and password which shall be used in accessing the system, and which shall be logged accordingly in the system; and
- 4.4.5 This access shall be limited to the workstation for retrieving the copy of the election results as transmitted by the Automated Counting Machines (ACMs).

5. Access to Data Center Equipment, System and Applications.

- 5.1 All equipment, computers, and network devices shall be installed and configured in a secure and closed network for access by identified equipment, computers, network devices and authorized personnel only;
- 5.2 All explicitly authorized personnel with Level II access shall be allowed access to Data Center equipment, system, and applications according to the delegated duties and responsibilities of each from the Commission *En Banc*;
 - 5.2.1 The specific duties and responsibilities of each Level II access personnel shall be written down and formally accepted by the person concerned to signify confirmation of understanding; and
 - 5.2.2 For this purpose, all Data Center systems and applications, including all scripts and software tools, shall be listed in a systems inventory with a short description of the use of each, together with the names of the personnel that are allowed access to each, including the specific access right and privilege allowed for each per personnel.
- 5.3 All system rights and privileges for each Level II access personnel to be provided by the Solution Provider Unit Head shall be validated by the SETS 2025 Unit Head for configuration by the designated Systems Administrator and shall be made known to all Level II access personnel for review, information, and monitoring;
 - 5.3.1 All lacking, incorrect, or inappropriately assigned system rights and privileges shall be brought to the attention of the SETS 2025

Unit Head and Solution Provider Unit Head by the concerned Data Center personnel; and

- 5.3.2 The appropriate correction to the system rights and privileges shall be performed by the designated Systems Administrator upon the direction of the Solution Provider Unit Head and validation of the SETS 2025 Unit Head.
- 5.4 All Data Center equipment, including computers and network appliances, shall be used only for purposes directly related to the implementation of the SETS 2025 Project, including operation and monitoring activities;
- 5.5 No public internet access connection shall be allowed within the SETS 2025 network except for the VPN connections specifically indicated in the contract for the SETS 2025 Project;
- 5.6 Only approved systems, tools, scripts, third party applications, and applications and systems developed and provided by the Solutions Provider, as listed in the above-named systems inventory, shall be used in the Data Centers;
- 5.7 Each authorized user shall be identified in the system with their own unique usernames and password;
 - 5.7.1 Each access by an authorized user shall be recorded in the system's immutable log.
 - 5.7.1.1 The system logs shall be monitored for availability and correctness by the Systems Administrator; and
 - 5.7.1.2 The system logs shall always be readily made available for audit purposes upon direction of the SETS 2025 Project Director.
- 5.8 The Two-Person-Rule or Split-Password shall be implemented in all systems, applications, and database in the Data Centers;
 - 5.8.1 The split-password shall be provided and maintained in secrecy by a designated COMELEC personnel and a designated Solutions Provider personnel; and
 - 5.8.2 The designated COMELEC and Solutions Provider personnel shall not share his/her half of the split password with each other.
- 5.9 All activities to be performed in the Data Centers during configuration, testing, final setup and implementation shall be in accordance with the SETS 2025 contract and shall be approved by the Commission *En Banc*;

- 5.9.1 All activities shall be reviewed for completeness and accuracy by the SETS 2025 Project Director and PMO Director;
- 5.9.2 There shall be a lock down point in the setup of the Data Centers for use on Election Day after the Final Testing and Sealing (FTS) of the ACM wherein no changes can be made in the systems' configurations. The Escalation Protocol as defined in the SETS 2025 contract will serve as a guide should there be a need for a change after the lock down point; and
 - 5.9.2.1 The execution of the lock down point in the Media Site shall be witnessed by political party representatives, subject to the signing of the appropriate confirmation documentation; and
 - 5.9.2.2 Initialization by the Commission *En Banc* shall be performed at all Data Centers including the Results Website.
- 5.9.3 Any activity immediately after the FTS of the ACM up to the proclamation process that is not included in the SETS 2025 contract shall not be executed but shall be formally cleared by the PMO Project Director with the Commission *En Banc* for authorization purposes.
 - 5.9.3.1 The SETS 2025 Project Director shall formally instruct the Unit Head on the appropriate action to take; and
 - 5.9.3.2 The concerned Unit Head shall formally report the action taken to the SETS 2025 Project Director immediately after implementing the instruction.
- 5.10 All equipment that shall be brought outside of the Data Center shall be subject to the approval of the Commission *En Banc* upon the recommendation of the PMO Director thru the SETS 2025 Project Director;
- 5.11 All equipment that shall be brought outside shall not contain any system or election data, if applicable;
 - 5.11.1 For this reason, all data in the Data Center equipment that has been approved for removal shall be backed up, with redundancy, to removable data storage devices.
 - 5.11.1.1 Back-up shall be performed by COMELEC with the assistance of the Solutions Provider. The copy of the back-up shall only be provided to COMELEC. There shall be no other copy of the back-up to be reproduced.
 - 5.11.1.2 All system shall be wiped out from all concerned workstations and/or servers accordingly.

5.11.1.3 The conduct of the system removal from the equipment to be removed from the Data center shall be formally attested to by the SETS 2025 Unit Head, together with the authorized representative of the Commission *En Banc*, and the authorized Solutions Provider representative.

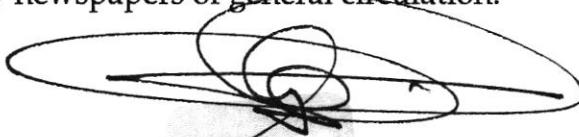
5.11.2 After data backup with redundancy, the data in the storage device of the concerned equipment shall be completely removed from the said storage device.

5.11.2.1 The conduct of the backing up and removal of data from the equipment to be removed from the Data center shall be formally attested to by the SETS 2025 Unit Head, together with the authorized representative of the Commission *En Banc*, and the authorized Solutions Provider representative.

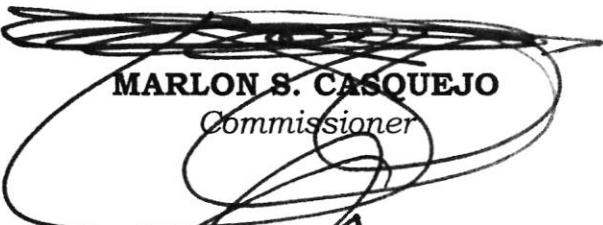
5.11.3 The data backup, including the redundant backup, shall be stored and secured by the SETS 2025 Project Director or by his authorized representative.

SECTION 11. Effectivity - This Resolution shall take effect immediately after its publication in two (2) daily newspapers of general circulation.

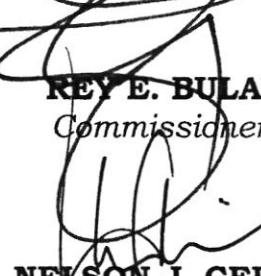
SO ORDERED.


GEORGE ERWIN M. GARCIA
Chairman


SOCORRO B. INTING
Commissioner


MARLON S. CASQUEJO
Commissioner


AIMEE P. FEROLINO
Commissioner

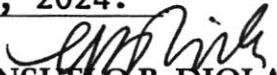

KEY E. BULAY
Commissioner


ERNESTO FERDINAND P. MACEDA, JR.
Commissioner


NELSON J. CELIS
Commissioner

CERTIFICATION

APPROVED for publication, November 20, 2024.


CONSUELO B. DIOLA
Director IV
Office of the Commission Secretary

This Resolution can be verified at this number (02)85272987; email address comsec@comelec.gov.ph