


I MINA' TRENTA NA LIHESLATURAN GUÅHAN
2009 (FIRST) Regular Session

Bill No. 30 (COR)

Introduced by:

Ray Tenorio 

AN ACT TO ADD A NEW CHAPTER 25 TO 5GCA RELATIVE
CREATING THE “INFORMATION SECURITY
MANAGEMENT ACT”.

2009 JAN -5 PM 12:59

1 BE IT ENACTED BY THE PEOPLE OF GUAM:

2
3 Section 1. A new Chapter 25 is hereby *added* to 5GCA to read:

4
5 Chapter 25

6 Information Security Management Act

7
8 §25101. Legislative Findings and Intent. *I Liheslaturan Guåhan* finds,
9 determines, and declares that:

10
11 (a) Communication and information resources in the various public agencies of the
12 Government of Guam are strategic and vital assets belonging to the people of
13 Guam. Coordinated efforts and a sense of urgency are necessary to protect these
14 assets against unauthorized access, disclosure, use, and modification or
15 destruction, whether accidental or deliberate, as well as to assure the
16 confidentiality, integrity, and availability of information.

17

1 (b) The Government of Guam has a duty to Guam citizens to ensure that the
2 information entrusted to public agencies is safe, secure, and protected from
3 unauthorized access, unauthorized use, or destruction.

4
5 (c) Securing the Government of Guam’s communication and information resources
6 is a Government-wide imperative requiring a coordinated and shared effort from
7 all departments, agencies, instrumentalities, public corporations and branches of
8 the Government of Guam and a long term commitment to funding that ensures the
9 success of such efforts.

10
11 (d) Risks to communication and information resources must be managed, and the
12 integrity of data and the source, destination, and processes applied to data must be
13 assured.

14
15 (e) Information security standards, policies, and guidelines must be promulgated
16 and implemented throughout public agencies to ensure the development and
17 maintenance of minimum information security controls to protect communication
18 and information resources that support the operations and assets of those agencies.

19
20 **§25102. Definitions.** As used in this Chapter, unless the context otherwise
21 requires:

22
23 (1) "AVAILABILITY" means the timely and reliable access to and use of
24 information created, generated, collected, or maintained by a public agency.

1 (2) "COMMUNICATION AND INFORMATION RESOURCES" shall have the
2 same meaning as applied to procedures, equipment, and software that are
3 designed, built, operated, and maintained to collect, record, process, store,
4 retrieve, display, and transmit, information. The term also includes associated
5 personnel including consultants and contractors.

6
7 (3) "CONFIDENTIALITY" means the preservation of authorized restrictions on
8 information access and disclosure, including the means for protecting personal
9 privacy and proprietary information.

10
11 (4) "INFORMATION SECURITY" means the protection of communication and
12 information resources from unauthorized access, use, disclosure, disruption,
13 modification, or destruction in order to:

14
15 (a) Prevent improper information modification or destruction;

16
17 (b) Preserve authorized restrictions on information access and disclosure;

18
19 (c) Ensure timely and reliable access to and use of information; and

20
21 (d) Maintain the confidentiality, integrity, and availability of information.

22
23 (5) "INFORMATION SECURITY PLAN" means the plan developed by a public
24 agency in accordance with this statute.

1 (6) "INSTITUTION OF HIGHER EDUCATION" means a Government of Guam-
2 supported institution of higher education.

3
4 (7) "INTEGRITY" means the prevention of improper information modification or
5 destruction and ensuring information nonrepudiation and authenticity.

6
7 (8) "PUBLIC AGENCY" means every Government office, whether legislative,
8 executive, or judicial, and all of its respective offices, departments, divisions,
9 commissions, boards, bureaus, and institutions.

10
11 (9) "SECURITY INCIDENT" means an accidental or deliberative event that
12 results in or constitutes an imminent threat of the unauthorized access, loss,
13 disclosure, modification, disruption, or destruction of communication and
14 information resources.

15
16 **§25103. Chief Information Security Officer - duties and responsibilities.**

17 (1) *I Maga Lahen Guahan* shall appoint a chief information security officer who
18 shall serve at the pleasure of *I Maga Lahi*. The officer shall exhibit a background
19 and expertise in the security and risk management for communications and
20 information resources. In the event the officer is unavailable to perform the duties
21 and responsibilities under this Chapter, all powers and authority granted to the
22 officer may be exercised by the Director of Administration or other person
23 designated by *I Maga Lahi*.

24
25 (2) The Chief Information Security Officer shall:

1 (a) Develop and assist in the update of information security procedures,
2 standards, and guidelines for all public agencies.

3
4 (b) Promulgate rules pursuant to 5GCA: Chapter 9;

5
6 (c) Ensure the incorporation of and compliance with information security
7 policies, standards, and guidelines in the information security plans
8 developed by public agencies in accordance with this Chapter;

9
10 (d) Direct information security audits and assessments in public agencies in
11 order to ensure program compliance and adjustments;

12
13 (e) Establish and direct a risk management process to identify information
14 security risks in public agencies and deploy risk mitigation strategies,
15 processes, and procedures;

16
17 (f) Annually review and approve the information security plans of public
18 agencies;

19
20 (g) Conduct information security awareness and training programs; and

21
22 (h) In coordination and consultation with the Bureau of Budget and
23 Management Research and the Director of Administration or Designee,
24 review public agency budget requests related to information security
25 systems and make recommendations on such budget requests for
26 Government agencies.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

§25104. Public agencies - information security plans.

(1) On or before each new fiscal year, each public agency shall develop an information security plan utilizing the information security policies, standards, and guidelines developed by the Chief Information Security Officer. The information security plan shall provide information security for the communication and information resources that support the operations and assets of the public agency.

(2) The Information Security Plan shall include:

(a) Periodic assessments of the risk and magnitude of the harm that could result from a security incident;

(b) A process for providing adequate information security for the communication and information resources of the public agency;

(c) Conduct periodic security awareness training to inform the employees and users of the public agency’s communication and information resources about information security risks and the responsibility of employees and users to comply with agency policies, standards, and procedures designed to reduce those risks;

(d) Periodic vulnerability assessment testing and evaluation of the effectiveness of information security for the public agency, which shall be performed not less than annually;

1 (e) A process for detecting, reporting, and responding to security incidents
2 consistent with the information security standards, policies, and guidelines
3 issued by the chief information security officer; and
4

5 (f) Plans and procedures to ensure the continuity of operations for
6 information resources that support the operations and assets of the public
7 agency in the event of a security incident.
8

9 (3) On or before each new fiscal year each public agency shall submit the
10 information security plan developed pursuant to this section to the chief
11 information security officer for approval.
12

13 (4) In the event that a public agency fails to submit to the chief information
14 security officer and information security plan on or before the new fiscal year, or
15 such plan is disapproved by the chief information security officer, the officer shall
16 notify the governor and the head and chief information officer of the public
17 agency of noncompliance with this section. If no plan has been approved within
18 the three subsequent months, the officer shall be authorized to temporarily
19 discontinue or suspend the operation of a public agency's communication and
20 information resources until such plan has been submitted to or is approved by the
21 officer.
22

23 (5) An information security plan may provide for a phase-in period not to exceed
24 three years. An implementation schedule for the phase-in period shall be included
25 in such a plan. Any phase-in period pursuant to this subsection shall be completed
26 by the current year plus three (3) years.

1

2 (6) On or before the new fiscal year, and on or before July 1 of each subsequent
3 year, the director or head of each public agency shall report to the chief
4 information security officer on the development, implementation, and, if
5 applicable, compliance with the phase-in schedule of the public agency's
6 information security plan.

7

8 **§25105. Reporting.** The chief information security officer shall report to *I Maga*
9 *Lahi* and *I Liheslatura* on an annual basis concerning the implementation of the
10 provisions of this plan.