(ISO 27001: 2013)
Contents

Information Security Management Systems (ISMS) Manual ................................................................. 1
1 Scope .................................................................................................................................................. 4
2 Normative references ......................................................................................................................... 4
3 Terms and definitions ........................................................................................................................ 4
4 Context of the organization ............................................................................................................ 4
   4.1 Understanding the organization and its context ........................................................................ 4
   4.2 Understanding the needs and expectations of interested parties ........................................... 4
   4.3 Determining the scope of the information security management system ............................... 5
   4.4 Information Security Management System .............................................................................. 5
5 Leadership .......................................................................................................................................... 5
   5.1 Leadership and commitment .................................................................................................. 5
   5.2 Policy ....................................................................................................................................... 6
   5.3 Organizational roles, responsibilities and authorities ............................................................. 6
6 Planning ............................................................................................................................................. 6
   6.1 Actions to address risks and opportunities ............................................................................. 6
       6.1.1 General ............................................................................................................................. 6
       6.1.2 Information Security Risk Assessment ........................................................................... 7
       6.1.3 Information Security Risk Treatment ............................................................................. 7
   6.2 Information security objectives and planning to achieve them ............................................ 7
7 Support ............................................................................................................................................. 8
   7.1 Resources .............................................................................................................................. 8
   7.2 Competence ............................................................................................................................ 8
   7.3 Awareness ............................................................................................................................... 8
   7.4 Communication ........................................................................................................................ 8
7.5 Documented information ............................................................................................................. 8
   7.5.1 General ............................................................................................................................. 8
   7.5.2 Creating and updating ......................................................................................................... 9
   7.5.3 Control of documented information .................................................................................... 9

All printed documents are uncontrolled copies. Please go to the link below for the most updated version.
https://sp.cog-ps.com/iso27k1/Shared%20Documents/A.%20Finalized%20Documents
8 Operation ......................................................................................................................... 9
  8.1 Operational planning and control.............................................................................. 9
  8.2 Information Security Risk Assessment...................................................................... 10
  8.3 Information Security Risk Treatment......................................................................... 10
9 Performance evaluation................................................................................................... 10
  9.1 Monitoring, measurement, analysis and evaluation...................................................... 10
  9.2 Internal audit.............................................................................................................. 10
  9.3 Management review.................................................................................................... 11
10 Improvement .................................................................................................................. 11
  10.1 Nonconformity and corrective action....................................................................... 11
  10.2 Continual improvement............................................................................................ 11
1 Scope
No content. This section is included to keep numbering for this manual consistent with the ISO/IEC 27001:2013 international standard. [Please see section 4.3 pertaining to Cognitive’s scope of registration.]

2 Normative references
No content. This section is included to keep numbering for this manual consistent with the ISO/IEC 27001:2013 international standard.

3 Terms and definitions
For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Context of the organization
4.1 Understanding the organization and its context
Cognitive is a small business providing resources for Federal, State and Local municipal agencies as well as commercial and non-profit entities. As such, Cognitive may be granted access to privileged client information in order to perform contracted services. Due to the nature of services offered, Cognitive may be obligated to comply with legislative or statutory information security requirements specific to individual contracts. Additional contract-specific Information Security Management System (ISMS) measures may be required by any client, necessitating the application of additional ISMS processes or tailoring of current processes to meet customer requirements. In order to ensure appropriate information security measures are applied as necessary, Cognitive has implemented an Information Security program consistent with and conforming to the ISO/IEC 27001:2013 standard for Information Security Management.

4.2 Understanding the needs and expectations of interested parties
Interested parties relevant to the information security management system include Cognitive employees, Cognitive subcontractors, customer organizations and, if applicable, customer suppliers or subcontractors who have access to client information and who Cognitive may be required to interface with in the performance of service delivery.

While some legal, statutory or regulatory IS requirements are applicable to all interested parties, customer agreements may often contain contract or agency-specific IS requirements. Agency or contract-specific IS requirements are reviewed by Cognitive management prior to contract signing in order to ensure that the requirements are clearly stated, that all interested parties are in agreement as to the meaning of the stated requirements, and that Cognitive can meet the stated requirements.
4.3 Determining the scope of the information security management system

The scope of registration for ISO 27001-2013 encompasses the COGNITIVE headquarters location and ensuring information security within the boundaries of headquarters operations and is formally stated as follows:

The Information Security Management Systems (ISMS) which applies to the provision and management of cost-effective workforce and IT solutions to Federal, State, Local and commercial customers. This is in accordance with the Cognitive ISO 27001 Statement of Applicability (SOA), dated 08/05/2015.

When determining this scope, the following factors were considered:

a) the external and internal issues referred to in 4.1;
b) the requirements referred to in 4.2; and
c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

4.4 Information Security Management System

In accordance with the requirements of ISO/IEC 27001-2013, Cognitive has established and implemented this information security management system (ISMS), and established procedures to maintain and continually improve the system. The master document for the ISMS is this Information Security Management Plan, which follows the same format as the ISO/IEC 27001-2013 standard. If Cognitive’s response to a requirement can be adequately expressed in brief textual format, the response will be included within this manual. Otherwise, this manual will reference the appropriate documents and records, and provide pointers to those documents or records.

5 Leadership

5.1 Leadership and commitment

Top management is committed to providing effective information security and, through the implementation of this ISMS, has taken steps to:

a) ensure the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
b) ensure the integration of the information security management system requirements into the organization's processes;
c) ensure that the resources needed for the information security management system are available;
d) communicate the importance of effective information security management and of conforming to the information security management system requirements;
e) ensure that the information security management system achieves its intended outcome(s);
f) direct and support persons to contribute to the effectiveness of the information security management system;
g) promote continual improvement; and
h) support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.
5.2 Policy
Top management has established an information security policy that:
  a) is appropriate to the purpose of the organization;
  b) includes high-level information security objectives (see 6.2) and provides the framework for setting more detailed security objectives at a process level;
  c) includes a commitment to satisfy applicable requirements related to information security; and
  d) includes a commitment to continual improvement of the ISMS.

This information security policy is:
  e) available as documented information in the Cognitive document control system (DCS);
  f) communicated within the organization; and
  g) available to interested parties, when determined appropriate by the Cognitive CEO.

Ref: DCS #05-006-0006 Cognitive Information Security Policy

5.3 Organizational roles, responsibilities and authorities
Cognitive’s top management is responsible for ensuring that the responsibilities and authorities for roles relevant to information security are assigned and communicated. At present, the Operations Manager is the designated individual with responsibility and authority for:

  a) ensuring that the information security management system conforms to the requirements of the ISO/IEC 27001:2013 International Standard; and
  b) reporting on the performance of the information security management system.

As the company grows and additional qualified personnel become available, management has the authority to assign responsibility and authority for reporting on the performance of the ISMS to other qualified individuals.

Roles and responsibilities for specific processes are defined within the process document.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General
When planning for the information security management system, Cognitive considers the issues referred to in 4.1 and the requirements referred to in 4.2 and determines the risks and opportunities that need to be addressed to:
  a) ensure the information security management system can achieve its intended outcome(s);
  b) prevent, or reduce, undesired effects; and
  c) achieve continual improvement,
and plans:

d) actions to address these risks and opportunities; and
e) how to
1) integrate and implement the actions into its information security management system processes; and
2) evaluate the effectiveness of these actions.

Identification and analysis of risks and application of appropriate controls to manage identified risks are accomplished and recorded in the Cognitive Statement of Applicability and the Cognitive Risk Analysis and Treatment Plan.

Ref: DCS# 05-001-0016 Statement of Applicability
Ref: DCS# 05-001-0015 Risk Analysis and Treatment Plan

6.1.2 Information Security Risk Assessment
Cognitive has designed and implemented an information security risk assessment process that provides a consistent, repeatable risk assessment methodology conforming to the requirements of the ISO/IEC 27001:2013 standard. This process is accomplished through the structure of Cognitive Risk Analysis and Treatment Plan, and continued maintenance of the Plan.

Ref: DCS# 05-001-0015 Risk Analysis and Treatment Plan

6.1.3 Information Security Risk Treatment
The Cognitive Statement of Applicability and the Risk Analysis and Treatment Plan provide details concerning controls applied to manage IS risks. Both documents are reviewed at least annually by the designated risk owners to ensure that identified risks are still applicable to the organization, to ensure that applied controls continue to be adequate and effective, and to recommend actions to improve currently applied controls.

Ref: DCS# 05-001-0016 Statement of Applicability
Ref: DCS# 05-001-0015 Risk Analysis and Treatment Plan

6.2 Information security objectives and planning to achieve them
The organization has established information security objectives consistent with the Information Security Policy at relevant functions and levels. These objectives, as well as specific measurements and measurement methodologies and timeframes are defined in the IS Metrics Repository. Process owners are typically assigned responsibility and authority for measurement collection and reporting; otherwise responsible individuals or departments will be identified in the Metrics Repository.

Ref: DCS # 05-001-0010 Cognitive Metrics Repository
7 Support

7.1 Resources
Cognitive Executive Leadership is fully committed to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS. In addition to creating and institutionalizing a comprehensive information security system, has established management review processes to ensure that operation of the ISMS proceeds as planned, and that sufficient resources are dedicated to enable an efficient and proactive IS program. The Management Review Board (MRB) ensures that all stakeholders remain informed. Additionally, the MRB confirms and monitors proactive coordination of activities across integrated responsibilities.

Ref: DCS # 05-001-0001 Management Review Board Charter

7.2 Competence
Cognitive ensures that all personnel assigned to responsibilities defined in the ISMS are competent to perform the required tasks. Personnel are hired or contracted based on skills, competencies, and certifications appropriate to the position, and additional on-the-job or external formal training is provided as needs arise. Training records for employees are maintained by the HR department at Cognitive Headquarters.

Ref: Job descriptions
Ref: Training records
Ref: Personnel evaluations

7.3 Awareness
The company ensures that all relevant personnel are aware of the significance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives. Personnel are introduced to the ISMS and their information security responsibilities upon employment and are informed by management when changes to the ISMS are necessary. This ISMS Plan is available to employees as a guide to ISMS-related policies, plans, procedures and work instructions.

7.4 Communication
Cognitive’s Operations Manager, representing the MRB, ensures that affected employees and other stakeholders are informed via e-mail when additions, deletions or changes take place within the ISMS. Changed or updated documentation concerning the ISMS is posted in the DCS and made available to affected parties.

7.5 Documented information

7.5.1 General
Cognitive’s information security management system includes:

a) documented information required by the ISO/IEC 27001:2013 International Standard; and
b) documented information determined by the organization as being necessary for the effectiveness of the information security management system.

ISMS documentation is maintained in the company DCS.

### 7.5.2 Creating and updating

Process owners are responsible for the creation, review and updating of system documentation. This process is controlled via the Document Control Procedure.

**Ref:** DCS# 05-004-0001 Document Control Procedure

### 7.5.3 Control of documented information

Documented information required by the information security management system and by this International Standard is controlled via the Document Control Procedure and the DCS Master Listing to ensure:

- a) it is available and suitable for use, where and when it is needed; and
- b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

The Document Control Procedure provides direction and guidance for:

- c) distribution, access, retrieval and use;
- d) storage and preservation, including the preservation of legibility;
- e) control of changes (e.g. version control); and
- f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, is identified as appropriate, and also controlled via the Document Control Procedure.

**Ref:** DCS# 05-004-0001 Document Control Procedure

**Ref:** Record Document Control System Master Listing

Record control is managed via the Control of Records Procedure and encompasses control of records required by ISO 27001 and internal records necessary for the operation of the business. A Record Control System (RCS) is maintained by the CEO and recorded in the RCS Master Listing.

**Ref:** DCS# 05-004-0001 Document Control Procedure

**Ref:** Record Document Control System Master Listing

### 8 Operation

#### 8.1 Operational planning and control

The Cognitive Information Security Management System, under the direction of the CEO, and the Management Review Board (MRB), outlines the processes and resources necessary to secure company information from threats against privacy, productivity or intellectual property rights. Documented
internal audits and management reviews ensure that the processes are carried out as planned. The company has implemented a formal Change Management process to ensure controlled change. Outsourced processes are identified and controlled through supplier management processes and included in risk management.

Ref: DCS# 05-001-0004 Internal Audit Procedure
Ref: DCS# 05-001-0003 Management Review Procedure
Ref: DCS# 05-003-0003 Change Request Form
Ref: DCS# 05-006-0001 Supplier Management Process

8.2 Information Security Risk Assessment
Information Security risk assessments are performed annually. When significant changes are being considered, risks associated with the proposed change are identified and assessed as part of change management and, if appropriate, added to the Cognitive Risk Analysis and Treatment Plan.

Ref: DCS# 05-001-0015 Risk Analysis and Treatment Plan
Ref: DCS# 05-003-0003 Change Request Form

8.3 Information Security Risk Treatment
The risk treatment plan, analysis, controls applied and reviews are documented and recorded via the Risk Analysis and Treatment Plan and the Statement of Applicability.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation
The Operations Manager and Management Review Board evaluate the performance and effectiveness of the ISMS through management review of internal process audit results, and the collection and analysis of specific process measurements. Internal audit records are retained in RCS and specific process measures are recorded in and reported from the Metrics Repository. Process owners are responsible for collecting and reporting specific process measurements.

Ref: Records Internal audit
Ref: DCS # 05-001-0010 Cognitive Metrics Repository
Ref: Records Management Review

9.2 Internal audit
Scheduled internal ISMS audits are conducted periodically by qualified internal auditors following a documented, repeatable process conforming to ISO requirements for internal audit. When Cognitive personnel perform internal audits, supporting forms referenced below are prepared and used as applicable in conducting each audit in order to ensure conformance and generate required records.

Ref: DCS# 05-001-0004 Internal Audit Procedure
Ref: DCS# 05-001-0007 Internal Audit Plan
9.3 Management review
Management performs management reviews on a quarterly basis following the formally documented process referenced below. Agendas are prepared in advance using a standard template and meeting minutes are entered directly into the template. Meeting Minutes are retained in the RCS.

Ref: DCS# 05-001-0003 Management Review Procedure
Ref: DCS# 05-001-0002 Management Review Meeting Agenda Template
Ref: Records Management Review Meeting Minutes

10 Improvement

10.1 Nonconformity and corrective action
When a nonconformity is identified, the company must take appropriate action in order to maintain the effectiveness of the ISMS. Corrective actions are managed using formal change management and a Request for Change form flagged “Corrective Action”. Change activity is entered directly into the form and retained in RCS change management records.

Ref: DCS# 05-003-0003 Change Request Form

10.2 Continual improvement
Cognitive is committed to continually improving the suitability, adequacy and effectiveness of the information security management system. The ISMS is monitored, results are brought to MRB for review and analysis. When possible improvements are identified, they are investigated and acted upon under change management using a request for change flagged “Opportunity for Improvement”.

Ref: DCS# 05-003-0003 Change Request Form
Ref: Records Management Review Meeting Minutes