Contents

A.17 Information security aspects of business continuity management..... 1

1. Purpose..... 1

2. Scope..... 1

3. Objectives..... 1

4. Governing Laws & Regulations..... 1

5. Policy Statement..... 1

A.17.1.1 Planning Information Security Continuity..... 2

A.17.1.2 Implementing Information Security Continuity..... 2

A.17.1.3 Verify, Review & Evaluate Information Security Continuity..... 2

A.17.2.1 Availability of Information Processing Facilities..... 3

6. Non-Compliance..... 3

7. Exceptions..... 3

8. Revision History..... 3

A.17 Information security aspects of business continuity management

1. Purpose

Annex A.17 is about aspects of business continuity management of Information Security.

2. Scope

This policy applies to all workers, project workers, and outsider specialist co-ops who approach the association's data resources, frameworks, and basic business tasks.

3. Objectives

These are the objectives of this policy:

- Recognize and concentrate on fundamental business frameworks and activities.
- Design and implement business congruency strategies that restore fundamental business processes and infrastructure.
- Ensure the timely reaffirmation and recovery of fundamental concepts and frameworks.
- To ensure their feasibility, lead normal testing and a business coherence study will be conducted.
- Ensure that every employee, worker-for-hire, and outside specialized cooperative is aware of their responsibilities in a security incident or disaster.

4. Governing Laws & Regulations

Guidance	Section
ISO27001:2013	A.17 (A.17.1, A.17.2)

5. Policy Statement

During difficult circumstances, the organization is committed to ensuring the advancement of data security across the board. The organization should focus on implementing an extensive data security the board framework that addresses the data security aspects of business congruity with the board because they understand how important business progression the executives are in ensuring the longevity and success of the company.

A.17.1.1 Planning Information Security Continuity

The executive's policy and strategies that cover the information security aspects of business advancement will be developed and maintained by this company. They should make sure that the policies and procedures are reviewed frequently, shared with the appropriate parties, and occasionally put to the test. The organization can then archive the agreement in whatever subtlety is required to indicate it understands those concerns and the means required to handle them. This comes after considering the many occasions and situations that should be anticipated.

A.17.1.2 Implementing Information Security Continuity

- The organization must plan, track, implement, and maintain cycles, systems, and controls to ensure the desired level of coherence for data security in trying conditions.
- When requirements are identified, the organization should put in place strategies, tactics, and other physical or technical controls that are adequate and proportionate to achieve those requirements.
- Illustration of the responsibilities, activities, owners, timetables, and relieving labor to be accepted (previous risks and active arrangements, like emergency exchanges).
- To ensure that the appropriate authority is notified successfully and as soon as feasible when an event becomes more dangerous, an administrative structure and pertinent escalating trigger points should be identified.

A.17.1.3 Verify, Review & Evaluate Information Security Continuity

- To ensure that the controls are valid and effective under these conditions, the organization should periodically review the layout and implementation of the data security coherence controls.
- To ensure that the measures implemented for data security congruity are kept up with against changes in the industry, technological advancements, and risk levels, they should be periodically tested, investigated, and assessed.
- The assessor will want evidence of Occasional testing of plans and controls; Logs of plan development and the moves initiated through to goal, and lessons learned; and intermittent audit and change of the board to ensure that plans are maintained against change.

A.17.2.1 Availability of Information Processing Facilities

A good control shows how data handling operations are carried out in a way that is sufficiently overtly repetitive to satisfy accessibility requirements. Overt repetition refers to using copy equipment frequently to ensure the accessibility of data handling frameworks. On the odd chance that even one item fails, there will be surplus things that will take precedence, is the rule.

The organization should take the necessary precautions, such as secure reinforcement, recovery techniques, and the occurrence of the board, to ensure the accessibility of data processing offices. Representatives of the BCM plan should receive training and awareness campaigns to ensure its resilience.

6. Non-Compliance

Non-Compliance with this policy must result in disciplinary action, including termination of employment or an agreement. The organization should take the necessary precautions to reduce the risks associated with non-compliance.

7. Exceptions

The Chief Information Security Official (CISO) or their designee should support and document any exceptions to this policy in writing. Before approving the special instance, the CISO or their designee will assess how the exemption would affect the organization's data security and business coherence frameworks. The important partners will be informed of the exemption. The organization will take the necessary steps to reduce the risks of the unique case.

8. Revision History

Version ID	Date of Change	Author	Rationale