الاتصالات المتكاملة
INTEGRATED TELECOM

ITC PII Security Policy

Version 1.0

Effective Date: 10th December 2019

الاتصالات المتكاملة
INTEGRATED TELECOM

Contents

الاتصالات المتكاملة
INTEGRATED TELECOM

PII SECURITY POLICY STATEMENT

The management of **Integrated Telecom Company** is committed for meeting the requirement, maintaining and continuously improving effective personally identifiable information (PII) security that safeguards information assets as well as the intellectual properties of ITC and clients.

We shall:

- Ensure compliance with applicable PII protection legislation and the contractual terms agreed between ITC and a public cloud PII processor and its clients (cloud service customers).
- Put measures in place to make relevant staff aware of the possible consequences on the public cloud PII processor, on the staff member and on the PII principal of breaching privacy or security rules and procedures, especially those addressing the handling of PII.
- Treat, for the purposes of secure disposal or re-use, equipment containing storage media that may possibly contain PII, as though it does.
- Provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

Identification of all PII residing in ITC environment

An organization cannot properly protect PII it does not know about. ITC follows this broad definition of PII to identify as many potential sources of PII as possible (e.g., databases, shared network drives, backup tapes, contractor sites). PII is — any information about an individual maintained by ITC, including

1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII at ITC shall include, but will not be limited to

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as national identity card number (SID), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry).
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

الاتصالات المتكاملة
INTEGRATED TELECOM

Minimization of the use, collection, and retention of PII

ITC shall minimize the use, collection and retention of PII to what is strictly necessary to accomplish its business purpose and mission. ITC shall, thereby, greatly reduce the likelihood of harm caused by a breach involving PII.

ITC shall –

- Regularly review current holdings of PII and ensure they are accurate, relevant, timely, and complete;
- Reduce PII holdings to the minimum necessary for proper performance of its functions;
- Develop a schedule for periodic review of PII holdings;
- Establish a plan to eliminate the unnecessary collection and use of SIDs.
- Follow a policy in respect of the return, transfer and/or disposal of PII and shall make this policy available to its cloud service customers.

ITC shall ensure that –

- PII to be processed under a contract is not processed for any purpose independent of the instructions of its cloud service customer
- PII processed under a contract is not used by it for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.
- Temporary files and documents are erased or destroyed within a specified, documented period
- The contract between ITC, as the public cloud PII processor, and the cloud service customer requires ITC to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.
- Disclosures of PII to third parties is recorded, including what PII has been disclosed, to whom and at what time.
- The use of sub-contractors by ITC, as the public cloud PII processor, to process PII should be disclosed to the relevant cloud service customers before their use
- ITC, as the public cloud PII processor, promptly notifies the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.
- Copies of security policies and operating procedures are retained for a specified, documented period upon replacement (including updating).
- Individuals under its control with access to PII are subject to a confidentiality obligation
- The creation of hardcopy material displaying PII is restricted
- There is a procedure for, and a log of, data restoration efforts

- PII on media leaving the premises of ITC is subject to an authorization procedure and should not be accessible to anyone other than authorized personnel

- Portable physical media and portable devices that do not permit encryption are not used except where it is unavoidable, and any use of such portable media and devices should be documented

- PII that is transmitted over public data-transmission networks is encrypted prior to transmission

- Where hardcopy materials are destroyed, they are destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

- If more than one individual has access to stored PII, then they each have a distinct user ID for identification, authentication and authorization purposes

- An up-to-date record of the users or profiles of users who have authorized access to the information system is maintained

- De-activated or expired user IDs are not granted to other individuals

- Contracts between the cloud service customer and ITC specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.

- Contracts between ITC, as the public cloud PII processor, and any sub-contractors that process PII specifies minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.

- Whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

- The countries in which PII might possibly be stored are specified and documented.

- PII transmitted using a data-transmission network is subject to appropriate controls designed to ensure that data reaches its intended destination

Categorization of PII

PII in ITC shall be evaluated to determine its PII confidentiality impact level so that appropriate safeguards can be applied to the PII.

The PII confidentiality impact level shall be rated as low, moderate, or high to indicate the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

ITC shall use the following factors to determine the PII confidentiality impact level.

Identifiability

ITC shall evaluate how easily PII can be used to identify specific individuals. For example, a SID uniquely and directly identifies an individual, whereas a telephone area code identifies a set of people.

Quantity of PII

ITC shall consider how many individuals can be identified from the PII. Breaches of 25 records and 25 million records may have different impacts. The PII confidentiality impact level should only be raised and not lowered based on this factor.

Data Field Sensitivity

ITC shall evaluate the sensitivity of each individual PII data field. For example, an individual's SID or financial account number is generally more sensitive than an individual's phone number or ZIP code.

ITC shall also consider how many individuals can be identified from the PII. Breaches of 25 records and 25 million records may have different impacts. The PII confidentiality impact level shall only be raised and not lowered based on this factor.

ITC shall also evaluate the sensitivity of the PII data fields when combined.

Context of Use

ITC shall evaluate the context of use -- the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The context of use may cause the same PII data elements to be assigned different PII confidentiality impact levels based on their use. For example, suppose that ITC has two lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization, and the second list is people who work undercover in law enforcement. If the confidentiality of the lists is breached, the potential impacts to the affected individuals and to the organization are significantly different for each list.

Obligations to Protect Confidentiality

If ITC is subject to any obligations to protect PII, it shall consider such obligations when determining the PII confidentiality impact level. Obligations to protect generally include laws, regulations, or other mandates.

Access to and Location of PII

ITC shall take into consideration the nature of authorized access to and the location of PII. When PII is accessed more often or by more people and systems, or the PII is regularly transmitted or transported offsite, then there are more opportunities to compromise the confidentiality of the PII.

Application of Safeguards for PII based on the PII Confidentiality Impact Level

Since all PII cannot be protected in the same way, ITC may apply appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level.

ITC may do the following operational safeguards, privacy-specific safeguards, and security controls as appropriate.

Creating Policies and Procedures

ITC shall develop comprehensive policies and procedures for protecting the confidentiality of PII.

Conducting Training

ITC shall reduce the possibility that PII will be accessed, used, or disclosed inappropriately by requiring that all individuals receive appropriate training before being granted access to systems containing PII.

De-Identifying PII

ITC may de-identify records by removing enough PII such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. De-identified records can be used when full records are not necessary, such as for examinations of correlations and trends.

Using Access Enforcement

ITC may control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).

Implementing Access Control for Mobile Devices

ITC may prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher risk than non-portable devices.

Providing Transmission Confidentiality

ITC may protect the confidentiality of transmitted PII. This may be accomplished by encrypting the communications or by encrypting the information before it is transmitted.

Auditing Events

ITC may monitor events that affect the confidentiality of PII, such as inappropriate access to PII.

Transfer of PII

Whenever physical media are used for information transfer, a system shall be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where possible, cloud service customers shall be asked to put additional measures in place (such as encryption) to ensure that the data can only be accessed at the point of destination and not en route.

Independent Evidence of Information Security

In cases where individual cloud service customer audits are impractical or may increase risks to security, ITC , as the public cloud PII processor shall make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent

evidence that information security is implemented and operated in accordance with the public cloud PII processor's policies and procedures.

Incident response plan to handle breaches involving PII

An information security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place

Breaches involving PII are hazardous to both individuals and organizations. Harm to individuals and organizations can be contained and minimized through the development of effective incident response plans for breaches involving PII.

ITC shall develop plans that include elements such as determining when and how individuals should be notified, how a breach should be reported, and whether to provide remedial services, such as credit monitoring, to affected individuals.

Coordination for PII

ITC shall establish close coordination among all officers responsible for PII. They may propose and implement technical security controls to enforce the confidentiality of PII. Close coordination of the relevant experts shall help prevent incidents that could result in the compromise and misuse of PII by ensuring proper interpretation and implementation of requirements.

Contractual Agreements for PII

Contractual agreements that involve PII shall clearly allocate responsibilities between ITC as the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question (e.g. a service of an IaaS, PaaS or SaaS category of the cloud computing reference architecture).

ITC, as a public cloud PII processor shall designate a point of contact for use by each of its cloud service customers regarding the processing of PII under the contract.

Event Logging for PII

A process shall be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, event logs shall record whether or not PII has been changed (added, modified or deleted) as a result of an event and by whom.

ITC, as the public cloud PII processor, shall define criteria regarding if, when and how log information can be made available to or usable by its cloud service customer. These procedures shall be made available to the cloud service customer.

Where a cloud service customer is permitted to access log records controlled by ITC as the public cloud PII processor, ITC shall ensure that the cloud service customer can only access records that relate to that respective cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.

ITC shall put in place measures to ensure that logged information is only used for its intended purposes.

ITC shall put in place a procedure to ensure that logged information is deleted within a specified and documented period.