GASEMBA CHRISTIAN CHILDREN'S FOUNDATION
"Creating a better future"

GASEMBA CHRISTIAN CHILDREN'S FOUNDATION

P.O.Box 900177 Jinja Uganda Email:gasembachildrensfoundation@gmail.com
gasembachildrensfoundation.org
+256 705067483/+256 788892880/+256 755627082

GASEMBA CHRISTIAN CHILDREN'S FOUNDATION

INFORMATION SECURITY POLICY FOR GASEMBA CHRISTIAN CHILDREN'S FOUNDATION

1. The Information Security Policy sets out the basis for Gasemba Christian children's foundation (GCCF) in protecting the confidentiality, integrity, and availability of its data, for classifying and handling confidential information, and for dealing with breaches of this Policy.

2. The Information Security Management System (ISMS) requires a comprehensive Information Security Policy document covering all areas of Information Security and, given the prevalence of automated information handling techniques, particularly in the area of ICT security. This document satisfies that requirement.

. **Purpose**

4. The management of Information Security is the reasonable selection and effective implementation of appropriate controls to protect critical organization information assets. Controls and management processes, coupled with the subsequent monitoring of their appropriateness and effectiveness, form the two primary elements of the Information Security programme. The three goals of Information Security include:

   a) Confidentiality
   b) Integrity
   c) Availability

5. The direction contained in Gasemba Christian children's foundation Human resource policy requires staff members shall exercise the utmost discretion with regard to all matters of official business. They shall not communicate to any Government, entity, person or any other source any information known to them by reason of their official position that they know or ought to have known has not been made public, except as appropriate in the normal course of their duties or by authorization of the Secretary-General. That direction is supported and implemented by this Policy.

6. This Policy sets out the basis for the protection of information, facilitating security management decisions, and directing those objectives which establish, promote, and ensure best Information Security controls and management within the GCCF working environment.

Scope

7. This Policy states broad management principles guiding the Information Security programme in place within GCCF. This Policy applies to all physical areas under the control of GCCF. Where other specific functional policies set more stringent requirements, they take precedence in those functional areas. This Information Security Policy shall be reviewed by the Information and Technology Management (ITM)/Bureau for Management Services (BMS) at regular intervals to ensure its continuing suitability, adequacy, and effectiveness.

8. Information security standards and information security related work instructions are **subordinate to** this Policy and provide more specific detail on implementation of this Information Security Policy.

Objectives

9. Establish the direction on and commitment to Information Security and ensure it is communicated, applied, and complied with throughout the organization. Further, to develop and implement Information Security architecture, to protect information assets from loss or misuse, and to mitigate the risk of financial, productivity, and reputation loss to GCCF.

10. The Information Security Policy consists of a principal declaration, which sets out the position on Information Security and defines three security principles upon which this Policy is formed, followed by nine supporting Policy Statements that expand upon those principles.

Principles

11. The GCCF recognizes that data and information (whether its own, or that entrusted to its care) are core to its ability to fulfill its mission.

12. The GCCF is fully committed to protecting information and the environments in which information is processed, transmitted and stored, consistent with the following security principles:

    a) Best practices in Information Security
    b) The value or level of sensitivity
    c) All applicable laws, policies, statutes, regulations, and contractual requirements

13. All GCCF staff and other authorized individuals or entities are responsible for maintaining appropriate control over information in their care and for bringing any potential threats to the confidentiality, integrity, or availability of that information to the attention of the appropriate management. Appropriate training and awareness programs will be available to support and reinforce this responsibility.

14. The following Policy Statements, support the Principal Declaration and define the compliance requirements of Information Security Policy management. The Statements address the following areas:

a) Asset Management

b) Human Resources Security

c) Physical and Environmental Security

d) Communications and Operations Management

e) Access Control

f) Information Systems Acquisition, Development and Maintenance

g) Information Security Incident Management

h) Business Continuity Management

i) Compliance

16. Adherence to both the Policy and the related Information Security standards is mandatory for all staff and other authorized individuals and entities, to be incorporated within relevant working procedures.

17. The ITM/BMS will undertake periodic monitoring and the Office of Audits and Investigations (OAI) will conduct periodic audits of GCCF units to confirm compliance with this Policy and related standards.

Asset Management

18. To achieve and maintain appropriate protection and control of GCCF information assets and to ensure that responsibility and accountability for this protection and control is properly vested in designated information owners/custodians. To ensure appropriate handling procedures are applied to important information assets.

Responsibility for Assets

19. All assets shall be clearly identified and an inventory of all important information-related assets drawn up and maintained for information security purpose.

Such important information-related assets for protection may include, but are not limited to:

a) Information: databases and data files, contracts and agreements, system documentation, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information

b) Software assets: application software, system software, development tools, and utilities

c) Physical assets: computer equipment, communication equipment, removable media, and other equipment

d) Services: computing and communications services, general utilities, e.g., heating, lighting, power, and air-conditioning

20. All information and assets associated with information systems shall be owned by a designated unit of GCCF. The designated owner (individual or entity that has approved management responsibility for controlling the custody, production, development, maintenance, use and security of the assets; Routine tasks may be delegated, e.g., to a custodian looking after the asset on a daily basis, but the responsibility remains with the owner) shall:

    a) Ensure that information and assets associated with information systems under their control are appropriately classified
    b) Periodically review access restrictions and classifications, taking into account applicable access policies

21. Rules and standards for the acceptable use of information and assets associated with information systems shall be identified, documented and implemented.

Information Classification

22. Information shall be classified or categorized in terms of its value, legal requirements, sensitivity, and criticality to the GCCF.

23. Appropriate procedures for labelling and handling sensitive information shall be developed and implemented. Such procedures may incorporate special handling qualifiers or other dissemination caveats such as "in-confidence" and/or "internal use only."

Human Resources Information Security

24. GCCF ensures that staff and other authorized individuals or entities understand their responsibilities and to reduce the risk of theft, fraud or misuse of facilities. Candidates for employment and all other authorized individuals should be adequately screened and detailed reference checks conducted, especially for sensitive jobs. Information security responsibilities should be addressed prior to employment, in job descriptions and in the terms and conditions of employment.

Prior to Employment

25. Security roles and responsibilities of all staff and other authorized individuals or entities of GCCF information assets shall be defined and documented in appropriate terms and conditions prior to employment or contract finalization, reflecting the requirements of this Policy.

26. Verification of critical information, including academic qualifications, languages, nationality, employment history and detailed reference checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant policies and procedures, and proportional to the organization's requirements, the classification of the information to be accessed, and the perceived risks. Reference checks shall take into

account all relevant privacy, protection of personal data and/or employment based established policies and procedures, and shall, as far as is permitted, include:

a) Availability of satisfactory references
b) A check (for completeness and accuracy) of the candidates Curriculum Vitae/Personal History Form
c) Confirmation of claimed academic and professional qualifications
d) An independent identity check
e) More detailed checks as appropriate

27. As part of their contractual obligation, GCCF staff conform to Rules and Regulation.

During Employment

28. All staff and other authorized individuals or entities using GCCF information assets shall apply security measures in accordance with all relevant GCCF regulations, rules, policies and procedures. All HR data, files and records are deemed sensitive and confidential. GCCF shall ensure that all staff and other authorized individuals or entities:

Are properly briefed on their Information Security roles and responsibilities prior to be granted access to sensitive information or information systems.

Are provided with sufficient guidelines outlining the information security expectations for their role within the GCCF.

29. All GCCF staff and, where relevant, other authorized individuals or entities, shall receive appropriate training and regular updates on Information Security-related policies and procedures as relevant to their function.

30. Any required disciplinary procedure resulting from a serious breach of Information Security assets or protocols shall be conducted in accordance with the relevant provisions of the GCCF Staff Regulations and Rules.

Staff Separation, Reassignment, and Termination

31. Responsibilities for performing employment separation, reassignment, and termination shall be clearly defined and assigned.

32. Staff and other authorized individuals or entities shall return all GCCF assets in their possession upon separation from employment, contract or agreement. The separation process shall formalize the return of all previously issued information assets.

33. The access rights of all staff and other authorized individuals or entities to information and information systems shall be removed or altered as appropriate upon separation or termination of their employment, contract or agreement, or adjusted upon reassignment.

Physical and Environmental Security

34. To ensure that GCCF premises, work areas, and information assets are adequately protected against identified risks to information assets. Critical or sensitive information systems should

be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls.

Information Assets

35. All staff and other authorized individuals or entities shall ensure that documents containing sensitive information are secured when not in use.

36. Sensitive information assets shall not be removed from GCCF premises without proper authorization.

Work Areas

37. Security perimeters (barriers such as walls, card-controlled entry gates and doors, and manned reception desks) shall be used to protect areas that contain information and information systems.

38. Security perimeters shall be clearly defined, and all security measures shall be implemented.

Equipment

39. Information systems shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

40. Information systems shall be protected from power failures and other disruptions caused by failures in supporting utilities. Such protection shall be integrated with business continuity planning (BCP) and disaster recovery (DR).

41. Information systems shall be correctly maintained to ensure continued availability and integrity. Only authorized maintenance staff or contractors shall perform maintenance, and adequate records of all maintenance shall be kept. Where appropriate, information should be cleared from storage equipment before maintenance is performed.

42. Security shall be applied to off-site information systems and equipment, taking into accounts the different risks of working outside GCCF premises. Such security may include measures to protect against casual theft when travelling, inappropriate use, or loss of confidentiality of information assets.

43. Information systems and equipment containing storage media shall be checked to ensure any sensitive data or licensed software has been removed or securely destroyed prior to disposal.

44. Information systems and equipment shall not be removed from GCCF premises without proper authorization.

Communications and Operations Management

45. To ensure the correct and secure operation of information systems, that key business and support processes incorporate effective Information Security controls, and that adequate operating procedures exist for the management and operation of GCCF information systems.

Operational Procedures and Responsibilities

46. Formal documented procedures shall be established, maintained, and made available for all activities involving information processing and communication facilities.

47. Changes to information systems and applications shall be subject to change management control. Change management procedures shall be developed with appropriate documentation to demonstrate compliance.

48. Appropriate segregation of duties and responsibilities shall be implemented to the greatest extent possible to reduce the possibility that any one individual can compromise an application, a policy, a procedure or activity, or to perform unauthorized or unintentional modifications to, or to misuse any information assets.

49. Development, test, and operational (production) facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.

Third Party Service Delivery Management

50. Service and delivery levels as well as security controls provided by third-party providers involved in supporting GCCF information processing or telecommunication services shall be monitored to ensure that services are implemented, operated, and maintained in accordance with contractual obligations.

51. Changes in the provision of third-party services shall be closely managed, taking into account the criticality of the information systems and processes involved and the re-assessment of all relevant risks.

System Planning and Acceptance

52. Acceptance criteria for new or upgraded information systems shall be established, and suitable tests of the system(s) carried out during development and prior to acceptance.

53. Existing information system resources shall be monitored and adjusted as necessary, and projections made of future capacity requirements, to ensure continued performance at the required levels.

Protection against Malicious and Mobile Code

54. Detective, preventive, and corrective controls, as well as appropriate user awareness procedures shall be implemented to protect against malicious code.

55. Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy.

Backup

56. Appropriate backup arrangements, including annual testing, shall be implemented and maintained to protect information and software and to ensure all critical information assets and processes can be recovered if required for any reason.

Network Security Management

57. Computer and communication networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for systems and applications using the network, including information in transit.

58. Security features, service levels, and management requirements of all network services, both internal and outsourced, shall be identified and included in all network services agreements.

Storage Media Handling

59. Procedures shall be established for the management of removable storage media, including procedures for the safe and secure disposal of storage media when no longer required.

60. Procedures shall be established for the handling and storage of information to protect against unauthorized disclosure or misuse.

Monitoring

61. Procedures for monitoring use of information systems shall be established and the results of the monitoring activities reviewed regularly. Monitoring shall be used to determine that actual usage complies with authorized usage.

62. Audit logs recording user activities, exceptions, and Information Security events shall be produced and kept for an agreed period to assist in possible investigations and/or access control monitoring. Logging facilities and log information shall be protected against tampering and unauthorized access.
    The system administrator and system operator activities should be logged. Faults should be logged, analysed and appropriate action taken. Where possible, event logs should record access including by whom, when, and which principal was accessed, and what (if any) changes were made (additions, modifications or deletions) as a result of the event. Measures such as controlling access should be put in place to ensure that logged information is only used as intended. A procedure, preferably automatic, should be put in place to ensure that logged information is either deleted or de-identified as specified in a corresponding retention schedule.

63. The clocks of all relevant information processing systems within the GCCF shall be synchronized with an agreed accurate time source.

Information exchange procedures

External Parties

64. External parties, in this policy, include partners and contractors. To maintain the security of the organization's information and information processing facilities that are accessed,

processed, communicated to, or managed by external parties and contractors, the following conditions apply:

a) The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access or sharing information with such entities.

b) Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements. Such agreements should also include provisions for ensuring that GCCF rules and privacy principles related to the processing are enforced.

65. There shall be no exchange of sensitive GCCF information with a third party without authorization and appropriate controls in place to protect the information from unauthorized disclosure. Agreements should be established for the exchange of information and software between GCCF and external parties.

Electronic Commerce and Business Information Systems

66. Information associated with the interconnection of business information systems shall be protected to prevent misuse or corruption. Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

67. Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. The integrity of information provided on publicly available system should be protected to prevent unauthorized modification.

Business Requirement for Access Control

68. To ensure appropriate restrictions on access to information, adequate access control shall be applied to the information assets to ensure access is available only to current members of staff (or other authorized individuals or entities) who require it in the course of their official duties and that the rights of user access take proper account of the type and level of sensitivity of the information concerned

Information System Access Control

69. GCCF information systems, networks, services, operating software, and applications shall be configured ensure that appropriate access control and authorization mechanisms are implemented, functional, and effective.

70. The use of utility programs that might be capable of overriding system or other access controls shall be restricted and tightly controlled.

71. Interactive sessions shall shut down after a defined period of inactivity, and restrictions on connection times shall be used to provide additional security for high-risk applications

Information Security in Networks

72. Automatic equipment identification shall be used to authenticate connections from equipment if it is important that the communications can only be initiated from a specific location or equipment.

73. Physical and logical access to diagnostic and configuration ports shall be controlled.

74. Groups of information services, users and information systems should be segregated on networks. For shared networks, especially those extending across GCCF's boundaries, the capability of users to connect to the network should be restricted to GCCF business purposes on a need-to-know basis.

75. Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the applications.

76. Access to operating systems should be controlled by a secure log-on procedure. All users should have a unique user ID for their personal use only and a suitable authentication technique used to authenticate users.

77. Sensitive systems should have a dedicated (isolated) computing environment.

78. A formal policy, operational plans and procedures should be developed and implemented for tele-working activities and appropriate security measures adopted to protect against the risks of using mobile computing and communication facilities.

Information Systems Acquisition, Development and Maintenance

79. Objectives - To ensure information systems (e.g., applications, infrastructures, services, etc.) are designed with security as an integral component and placed into production with all system-specific security requirements fully understood and implemented.

Security Requirements for Information Systems

80. New information systems and major system enhancements shall be formally presented to and approved by the ICT Board before being acquired or developed. New information systems and system enhancements shall undertake formal testing in a controlled environment with user acceptance testing (UAT) prior to their promotion to production status. Formal testing shall include appropriate testing of all security requirements to ensure both their correctness and adequacy. Tests shall be documented and test results shall be retained as information assets.

81. The security requirements of a new information system or system enhancement shall be identified and agreed upon prior to system development or procurement

82. Ownership responsibilities in respect to a new information system shall be agreed upon prior to its implementation.

83. Data validation controls shall be incorporated during development and maintenance of information systems to detect and prevent any corruption of information through input, processing, or output errors. Requirements for ensuring authenticity and protecting message

integrity in applications shall be identified, and appropriate controls identified and implemented.

Cryptographic Controls

84. The implementation of cryptographic controls during acquisition, development, and maintenance of information systems shall be managed and shall incorporate appropriate key management procedures.

Security of System Files

85. Procedures shall be implemented to control the installation of software on operational systems. Specific responsibilities for the installation of software on operational systems shall be defined and allocated to appropriately trained authorized users only. Operational software libraries shall be maintained and access to program source code shall be restricted.

Security in Development and Support Processes

86. All changes to production information systems (and their source code) shall be formally authorized and controlled to prevent the potential compromise of business processing and security arrangements. Adequate and documented testing of all changes shall be performed.

87. Before operating systems are changed, business critical applications shall be viewed and tested to ensure there is no adverse impact on organizational operations or security.

88. Outsourced software development shall be supervised and monitored by the appropriate GCCF unit(s).

Technical Vulnerability Management

89. Timely information about technical vulnerabilities of information systems being used shall be obtained, exposure to such vulnerabilities evaluated, and appropriate measures taken to address associated risks. Where possible, systems should be enabled with automated updates in order to keep the latest security patches installed on systems in an expedited manner.

90. The ITM monitors and conducts periodic assessments of risk to processes, information, systems and facilities shall be performed in light of changing threats and technical vulnerabilities.

Information Security Incident Management

91. Objectives - To ensure incidents affecting Information Security within GCCF are reported and responded to in a timely and effective manner to allow corrective action to be taken.

Reporting Information Security Incidents and Weaknesses

92. All staff members and other authorized individuals or entities are required to report suspected information security weaknesses or incidents to the GCCF ICT Security unit.

Management of Information Security Incidents and Improvements

93. The Information Security Section shall develop and maintain Information Security event reporting and escalation procedures to ensure that Information Security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

94. In cases where an Information Security incident may involve either legal action or an internal investigation, the Director, ITM will consult with the Office of Legal Services (OLS) and/or the Office of Audit and Investigation (OAI), in order to authorize the collection and retention of related evidence and its subsequent provision to the OLS and/or the OAI.

Business Continuity Management

95. Objective: To ensure that GCCF is equipped to react to disruptions of operations, and to ensure the timely resumption of critical business processes, following disasters or major failures of information systems.

Information Security Aspects of Business Continuity Management

96. To ensure business continuity, the ICT Disaster recovery standard policy is in place.

Compliance with Legal Requirements

97. To ensure compliance with applicable legal, statutory, regulatory, and contractual requirements, procedures shall be implemented to guide GCCF in terms of its obligations. Such obligations may be derived from, but are not limited to:

a) Decisions of GCCF policy-making organs
b) Administrative directives

Compliance with Security Policies and Standards

98. GCCF managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. Managers in Regional Hubs and Country Offices shall make an annual self-attestation that they are in compliance with this Information Security Policy and its related standards. The Director, ITM will make a similar statement on behalf of the GCCF Headquarters. Any non-compliance must be documented along with the reasons for non-compliance

Information Security Audit Considerations

99. Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to in advance, to minimize the risk of disruptions to business processes.

100. Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

Roles & Responsibilities

101. The Director, ITM is responsible for Information Security within GCCF.

102. The Chief Information Security Officer (CISO), ITM provides technical advisory support to the Director of ITM. CISO is responsible for governance of developing, implementing, maintaining and monitoring of privacy safeguards compliant with privacy objectives defined by the ITM clients.

The Information Security Programme

103. An Information Security programme exists within GCCF to ensure that there is clear responsibility and accountability, both within and across organizational units, for the management of Information Security. The Information Security programme consists of the policies, standards, work instructions, organizational units and individuals with security responsibilities and provides the structure as well as an effective mechanism for coordinating and managing Information Security for the organization.

104. In support of the Information Security programme, the ITM exercises its duties in the following areas:

   a) Evaluate potential risks, determine the requirements and recommend suitable countermeasures to manage risks, in areas relating to the handling and protection of information by the GCCF
   b) Organize and coordinate the training of staff members in the areas of operations, information, communications, authorized users, facility, and information technology-related security procedures to be followed while working with GCCF

105. By providing consultancy and support, and by performing ongoing reviews, the ITM will assist individual organizational units to comply with policies in support of the Information Security programme.

106. The ITM ICT Security shall also participate in the process of authorizing new information systems or applications to ensure that necessary security elements are considered and adequately addressed prior to the new system's approval for use by GCCF.

107. The Office of Audits and Investigations (OAI) shall provide the senior management of GCCF with a periodic independent assessment of the operation and effectiveness of the Information Security programme.

108. There will be regular Information Security Management Meetings consisting of staff members and contractors in GCCF who are key to implementing the information security programme.

Compliance

109. Failure to comply with this Policy without obtaining a prior waiver shall be dealt with in accordance with GCCF Staff Regulations and Rules, or as appropriate, the staff contractual terms.

Exceptions

110. Where an organizational unit is unable to meet a policy statement contained in this document, the Head of a unit shall obtain a waiver from the Director, ITM.

111. All waiver requests shall be viewed as temporary and carry a specific expiration date. They are subject to review by the Director, ITM.

112. If a waiver is no longer required before the expiration date or annual review, the Head of the unit shall inform or advise the Director, ITM

Personally Identifiable Information (PII)

113. ITM is designated as a PII processor for all corporate applications supported by the ITM. As such, ITM does not determine the purposes and means for processing PII. ITM is a privacy stakeholder that processes PII on behalf of and in accordance with the instructions of internal and external data subjects who act as PII controllers. ITM is committed to PII protection following GCCF Privacy Principles as well as provisions of the GCCF Personal Data Protection and Privacy Policy

114. The organization shall ensure, where relevant, that the contract to process PII addresses the organization's role in providing assistance with the customer's obligations, (taking into account the nature of processing and the information available to the organization).

115. The organization shall ensure that PII processed on behalf of a customer are only processed for the purposes expressed in the documented instructions of the customer.

116. The organization shall inform the customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.

117. The organization shall provide the customer with the appropriate information such that the customer can demonstrate compliance with their obligations. Also, the organization shall provide the customer with the means to comply with its obligations related to PII principals.

118. The organization shall determine and maintain the necessary records in support of demonstrating compliance with its obligations (as specified in the applicable contract) for the processing of PII carried out on behalf of a customer.

119. The organization shall ensure that temporary files created as a result of the processing of PII are disposed of (e.g., erased or destroyed) following documented procedures within a specified, documented period. Also, PII backup restorations shall be reported to the ITM Cybersecurity unit with at least:

- the name of the person responsible for the restoration;
- a description of the restored PII.

120. The organization shall provide the ability to return, transfer and/or disposal of PII in a secure manner. It shall also make its policy available to the customer.

121. The organization shall subject PII transmitted over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

122. The organization shall inform the customer in a timely manner of the basis for PII transfers between jurisdictions and of any intended changes in this regard, so that the customer has the ability to object to such changes or to terminate the contract.

123. The organization shall specify and document the countries and international organizations to which PII can possibly be transferred.

124. The organization shall record disclosures of PII to third parties, including what PII has been disclosed, to whom and when.

125. The organization shall notify the customer of any legally binding requests for disclosure of PII.

126. The organization shall reject any requests for PII disclosures that are not legally binding, consult the corresponding customer before making any PII disclosures and accepting any contractually agreed requests for PII disclosures that are authorized by the corresponding customer.

127. The organization shall disclose any use of subcontractors to process PII to the customer before use.

128. The organization shall only engage a subcontractor to process PII according to the customer contract. Where possible, a Non-disclosure Agreement that covers PII processing should be signed by the subcontractor.

129. The organization shall, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PII, thereby giving the customer the opportunity to object to such changes.

130. Systems and/or components related to the processing of PII should be designed following the principles of privacy by design and privacy by default, and to anticipate and facilitate the implementation of relevant controls, in particular such that the collection and processing of PII in those systems is limited to what is necessary for the identified purposes of the processing of PII. This requirement also applies to outsourced development.