Commentaries to the Draft Guiding Principles for Safe Havens for Archives at Risk

Table of Contents

Preamble

Archives/records provide irreplaceable materials for ongoing and future dealing with the past processes.

Dealing with the past refers to the processes addressing the rights of victims and societies as a whole to truth, justice, reparations and guarantees of non-recurrence in the aftermath of grave human rights violations and breaches of international humanitarian law.

The Guiding Principles for Safe Havens for Archives at Risk take into account the Universal Declaration of Archives, the rights of victims and societies enshrined in international law, namely in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the four Geneva Conventions.

The United Nations Set of Principles for the Protection and Promotion of Human Rights through Action to Combat Impunity, in Principles 14 to 18, refers to the special attention that archives/records should receive in dealing with the past. Archives/records in the framework of these Principles consist of any kind of material, which provides information relevant for dealing with the past processes. Such archives are often at risk of destruction or alteration for a number of reasons, including climate change, conscious and unconscious acts, neglect, or storage in inappropriate conditions.

In exceptional circumstances, the risk, which such archives face is so serious and immediate that their continued existence requires that the archives or security copies thereof are sent to a safe haven, if necessary even in another country. As this raises an array of ethical and practical issues, sending original archives or copies abroad should be considered only as a measure of last resort. In addition, removing original archives to a safe haven should, wherever feasible, be of a temporary nature.

Due to the concerns referred to above, such an action should always be based on a set of clearly defined principles. The Guiding Principles for Safe Havens for Archives at Risk provide guidance to sending and hosting institutions for situations in which the safeguarding of originals or security copies through relocation can contribute to dealing with the past processes. They are based on a wide range of existing international experiences.

A Definitions

Archives/records: Materials created or received by a person, family, or organization, public or private, in the conduct of their affairs and preserved because of the enduring value of the information they contain or as evidence of the functions and responsibilities of their creator.

Custody: Care and control, especially for security and preservation; guardianship.

Dealing with the Past: Dealing with the past refers to the processes addressing the rights of victims and societies as a whole to truth, justice, reparations and guarantees of non-recurrence in the aftermath of grave human rights violations and breaches of international humanitarian law.

Hosting institution: The term “hosting institution” refers to a governmental or non-governmental organization/ institution interested in or already offering a safe haven solution for archives/records at risk.

Sending institution: The term “sending institution” refers to a governmental or non-governmental organization/ institution or a person that has found or is looking for a safe haven for its archives/records.

B Principles for Safe Havens for Archives at Risk

General Principles

1. **Safe haven solutions should be implemented if archives/records that contribute to dealing with the past processes are at risk of destruction or alteration. *(Purpose of Dealing with the Past Principle)***

Commentary on Principle 1: Purpose of Dealing with the Past Principle

This principle specifies the overall purpose of this document, namely the safeguarding that contribute to dealing with the past processes.

This specification does not exclude that certain principles can also be applied to other types of archives at risk.

This principle is closely linked to definitions and principles of the United Nations Updated Set of principles for the protection and promotion of human rights through action to combat impunity (2005, E/CN.4/2005/102/Add.1) (hereinafter: Updated Set of principles against impunity). Accordingly, "archives that contribute to dealing with the past processes" can be defined in line with the Updated Set of principles against impunity as "collections of documents pertaining to violations of human rights and humanitarian law from sources including (a) national governmental agencies, particularly those that played significant roles in relation to human rights violations; (b) local agencies, such as police stations, that were involved in human rights violations; (c) State agencies, including the office of the prosecutor and the judiciary, that are involved in the protection of human rights; and (d) materials collected by truth commissions and other investigative bodies." (Definitions, page 6).

Principle 14 of the Updated Set of principles against impunity implies that "archives must be preserved in order to guarantee the right to know. Namely, "technical measures and penalties should be applied to prevent any removal, destruction, concealment or falsification of archives, especially for the purpose of ensuring the impunity of perpetrators of violations of human rights and/or humanitarian law".

A number of different risks threaten such archives, some of which are listed in the Preamble. The following list is not exhaustive:

- Natural risks: Fire, flooding, earthquake or other natural causes, caused by climate change or other grounds;
- Risks linked to the institutional environment: Inadequate or unstable buildings, bacteria, insects and rodents, mould and humidity, dust, pollution
- Risks linked to institutional deficiency: Lack of restoration/conservation capacity; neglect; administrative order; unauthorised destruction; theft; damage from use
- Other manmade risks: Civil disorder; armed conflict; military occupation; government action or inaction; change of regime

Several of the risks identified above derive from shortage of resources, absence of archival expertise, and the absence of awareness about the importance of managing archives for good governance, the protection of human rights, or poor administration in general. Such problems are capable of being

resolved locally in many cases. Four threats in particular, however, can - in certain circumstances - require the consideration of archival relocation to a different country: armed conflict; military occupation; repressive actions by government or non-government actors and recurrent, unavoidable natural risks (for example, sea rise due to climate change). These are the main circumstances covered by these Principles.

Concerning archives at risk due to armed conflict, military occupation and repressive actions, international humanitarian law establishes certain guidance. Article 1 of the 1954 Hague Convention for the Protection of Cultural Property in the event of Armed Conflict (hereinafter 1954 Hague Convention) prohibits the destruction of "manuscripts … and important collections of books or archives" and buildings such as "depositories of archives" in situations of armed conflict and occupation. This immunity can only been withdrawn, "in exceptional cases of unavoidable military necessity, and only for such time as that necessity continues" (Art. 11). The international protective emblem of the "blue shield" as defined in Art. 6 of the 1954 Hague Convention identifies structures, such as archives, that are not lawful targets in an armed conflict. However, in practice, this is often ignored by the belligerent parties. Armed conflict often disrupts all services including archival services. In active hostilities, especially when involving heavy artillery or bombing campaigns, and in urban areas, the risk of having archives destroyed is high. In certain contexts, armed conflict evolves in a way that allows the relocation of archives in a relatively organized manner based on respective contingency planning. However, in other circumstances the need for relocation may emerge suddenly without leaving time for well-organised measures. However, the duration of the need for relocation is finite: the archives can be returned to the place of origin when the conflict ends and rebuilding begins.

Both in armed conflict and authoritarian regimes non-government archives that are relevant for dealing with the past are threatened existentially. For an initial period, the non-governmental actors may not be viewed as a threat by the forces in power, but when the level of confrontation rises or when the regime becomes more repressive for different reasons, the danger to these archives increases. Then non-governmental actors may, for example, find their offices or private spaces raided and records seized or destroyed.

In situations of transitions, both government and non-government archives containing relevant information related to violations of international humanitarian and human rights law are at particular risk, since they are relevant for accountability and truth searching mechanisms.

2. A safe haven solution abroad shall only be implemented when it is deemed impossible to store the information safely within the country, especially when transferring originals. *(Last Resort Principle)*

Commentary on Principle 2: Last Resort Principle

This Principle underlines the importance finding solutions locally, before moving archives abroad, in particular original physical archives. Moving the original physical archives or the only known copy of a digital archive should be an option of last resort since its transfer is particularly critical, considering the enormous duty of care required and the increased importance to be clear on ownership. The

importance of this principle was underlined in the report of the Office of the UN High Commissioner for Human Rights on experiences of archives as a means to guarantee the right to the truth (2011).

To minimize the risk that important information is lost or destroyed, three options for protection and preservation exist: 1) Securing the archives where they are; 2) moving (digital or analogue) copies within the country or abroad; 3) moving the originals within the country or abroad, as a very last resort.

Generally, it is important that both state and non-state actors fulfil their responsibility to safeguard archives relevant for dealing with the past professionally. When the institution holding archives identifies a high risk to the holdings, strategies for the preservation of the archives and contingency plans with different phases should be put in place, if possible before the crisis occurs. Specific actions should be linked to each phase of a contingency plan (e.g. to phase green, to phase orange, and to phase red).

An archival census, survey or registry can be an important assistance to preventive contingency planning. The first step would be to assess the nature and volume of archives/records that face a particular risk. As the archives may be located in different geographical areas, some may not be easily accessible for security reasons. Once there is an overview of the existing materials, the institution must decide which of them to save. Often a vast quantity of materials in all physical forms in a number of different archives exist — increasingly in born-digital formats — and making choices about priorities for preservation is essential.

The Guiding Principles for Safe Havens for Archives at Risk lay specific focus on the options to move security copies of archives, either within a country from one institution to another or, as last resort, to an institution abroad. However, many of the Principles are also relevant when moving originals abroad or within the country or origin. Nevertheless, it is important to consider the difference in the implications of moving the original abroad and moving security copies.

The transfer of original physical items is possible, but it requires enough time and a small enough quantity for this to be an effective means of protection. The quantity of the archival material to be moved is thus a key factor. Institutions thinking about this option need to create and maintain a continuously updated list of those crucially important archives that are essential to evacuate in times of crisis, and the archivists need to know what and where the archives are that need to be moved first in an emergency. Preparation for moving can be done at a moderate speed initially, but as threats materialise, speed becomes urgent. Institutions or individuals creating records that they know are likely to be destroyed or confiscated need to develop a relationship with an external institution that can be trusted to provide secure storage for the materials, since raids on the office or house are unpredictable and hacking attacks on websites occur equally without warning. The duration of the need for external storage will be uncertain and indefinite, but when conditions change in the country, the archives can be returned to form part of the country's archival heritage.

High priority for relocation of original documents should be given to archives important for asserting or protecting human rights; e.g. archives that contain potentially important information for future dealing with the past processes. In addition, holdings that have intrinsic value need to be considered for relocation (that is, permanently valuable records that have qualities and characteristics that make the records in their original physical form the only acceptable form for preservation). These may include documentation of the establishment or continuing legal basis of a country or an agency or institution, records whose age provides a quality of uniqueness, or materials that are rare or have a rare aesthetic or artistic quality.

As well as assessing the intrinsic value of archives, the actors should also consider doing a valuation exercise, considering both different perspectives and the country's conditions. This assessment may include aspects related to the significance of the records in terms of their value in both social and community processes and the value they hold for future generations.

Another kind of archives at risk that require physical relocation are those threatened by irreversible nationwide natural conditions; e.g., due to climate change. Such archives require a long-term solution. Some archives are located in areas that will experience inexorable sea level rise, accompanied by an increase of storm surges and violent weather, assuming current climatic conditions are not altered. In such cases a permanent new location should be determined by the consensus of the affected persons.

If the archives at risk do not appear to have intrinsic value, copying or digitizing is an option. However, when making that decision, the institution needs to take into account the requirements of the judicial system that may use these materials as evidence. Depending on the procedural law that applies, in some countries only the original archives or a specific kind of copy (such as a certified true copy) have probative value. If the original materials are to be digitized, the institution must plan for sufficient time and perhaps legal assistance to make a digital copy that will meet the legal standard.

In contrast to original items, a duplicate either of born-digital archives or information in another medium/format that has been digitized can be stored in many parts of the world. A number of technical options allow for the safeguarding of digital archives. Since the developments in this field are rapid and the safety of different options is controversial, the Principles do not define technical solutions, but leave it to the sending and hosting institutions to define the solution that suits them best. Some of the options discussed in the expert group that drafted the Principles were the following:

- Remote storage in a cloud environment. If this option is chosen, the security vulnerabilities of the cloud must be addressed. As data protection and the security of the information are fundamental, the risk of hacking needs to be part of the assessment.
- Storage on a local server the host institution; i.e., a trusted digital repository.

3. The hosting institution should document all laws, policies, standards, processes, procedures and the means of verification to which they comply and make them available to the sending institution. *(Transparency Principle)*

Commentary on Principle 3: Transparency Principle

It is relevant for any institution sending archives at risk, be it in physical or digital form, to know exactly which laws, policies, standards, processes, procedures and means of verification apply to a potential hosting institution. This information is relevant for an informed decision and must be made available fully to the sending institution before or in the course of negotiating a safe haven solution/agreement.

This information should include potential possibilities to exempt the archival material at risk from the application of any or all of the hosting institution's laws, policies, processes, procedures and standards should the sending institution deem them undesirable or unnecessary. In some cases, for example, the safe physical storage of one or more copies of digital material may be sufficient to

provide the protection that the sending institution requires without the need for further archival or digital preservation actions, even if they might be required for public records in the host country.

4. **Any safe haven solution should be based on a written bilateral agreement between the sending and the hosting institution. The agreement should reflect the mutual understanding of the laws, policies and the procedures that will be applied to the materials of the sending institution. It should include the purpose, subject of the agreement, roles and responsibilities, liability, as well as judicial steps in case of disagreement. *(Legality and Agreement Principle)***

Commentary on Principle 4: Legality and agreement principle

It is essential that the legally binding agreement on any safe haven solution is in written form. If the sending and the hosting institutions are state institutions, this bilateral agreement will normally have the form of a treaty between the two countries. This includes transfer and other technical protocols; it is also desirable to have written documentation of the negotiations leading to the agreement.

It is important to assess carefully all applicable laws, policies and the procedures in both the country of the sending and of the hosting institution. Reference should be made to them in the written agreement.

As a minimum, the written agreement should include the purpose and the subject of the agreement, the roles and responsibilities of the contracting parties, possible liability settlements, as well as judicial steps in case of disagreement between the contracting parties. Judicial steps could also include recourse to arbitration.

Further, any agreement between a sending and a hosting institution should state clearly which laws would apply to the execution of the agreement in the case of conflict over the implementation of the provisions. Normally this will be the law of the country of the hosting institution, given that insecurity in the country of the sending institution is the reason for the relocation.

If the agreement exists in more than one language version, the agreement must also specify which version(s) will be the authoritative version for legal matters.

If the safe haven solution agreed upon contains financial commitments from either party to the agreement, the agreement must state such commitments clearly and in detail.

5. **The goals of the sending institution in seeking a safe haven for archives/records shall be paramount in determining how they are treated by the hosting institution. *(Main Goal Principle)***

Commentary on Principle 5: Main Goal Principle

This Principle embodies the idea that the sending institution is the owner of the material to be secured in a safe haven solution. The sending institution knows best what material is in danger and how it needs to be secured.

The sending institution, therefore, needs to be able to decide together with the hosting institution what the legal and technical framework of the safe haven solution should be, including but not limited to the access rules, the duration of the safe haven solution, and the level of technical and institutional security.

6. **The hosting institution should have a stated ethical code, transparently embedded into the institution's governance. Taking into account that archives/records relevant for dealing with the past processes often contain highly personal and sensitive information on victims and perpetrators of human rights violations, the hosting institution should be guided by the ideas of:**

   a) **Do no harm**

   b) **Conflict sensitivity**

   c) **Data protection and right to privacy. *(Ethics Principle)***

Commentary on Principle 6: Ethics Principle

The ethical code enshrined in this Principle should guide the negotiation, conclusion and implementation of any safe haven agreement.

Hosting and sending institutions should adhere to the Code of Ethics of the International Council on Archives, as well as the values underlying the ICA/UNESCO Universal Declaration on Archives, the ICA Principles of Access to Archives and the ICA Working Document on Basic Principles on the Role of Archivists and Records Managers in Support of Human Rights.

The principles of "do no harm" and conflict sensitive programming are used in peace building initiatives, deriving from the assumption that there is no neutral outside intervention and aid in contexts of conflict. Any outside intervention, including the one related to safeguarding archives at risk, can potentially cause harm. Therefore, all parties involved in finding a safe haven solution should be aware of potential harm and try to minimize factors causing harm by carefully assessing the impact of their decisions and acts. The concepts also embrace the hypothesis that conflict sensitive interventions can strengthen local capacities for peace, build on connectors that bring communities together, and reduce the divisions and sources of tensions that can lead to destructive conflict. Conflict sensitive interventions require a careful conflict and context analysis that examines how potential actions interact with the conflict, and a willingness to create options and redesign initiatives as well as careful reflection on staff conduct and organisational policies.

Archives relevant for dealing with the past processes often contain sensitive information about individuals, including victims and perpetrators. It is thus crucial that the hosting institution is aware of the potential danger of providing access to those archives. Throughout the process of providing a safe haven for archives at risk, the hosting institution should constantly consider the aspect to do no harm, to act in a conflict sensitive manner and to not lose sight of the main goal of data protection.

7. **Safe haven solutions shall be based on a fair agreement, acknowledging the potential asymmetrical nature of the relationship, including language barriers, mitigating the risks deriving therefrom and not taking advantage of the asymmetry. *(Fair Agreement Principle)***

Commentary on Principle 7: Fair Agreement Principle

In safe haven agreements, there is usually a certain asymmetry in the relationship between the sending and the hosting institution. Sending institutions are looking for safe havens for their archives precisely because they are usually exposed to political violence and may operate in an unpredictable, unreliable or non-independent, biased legal system. Further, sending institutions may not be economically sustainable, may have very limited capacity, language challenges, may use outdated and/or unappropriated standards or techniques, etc.

Consequently, it is important that hosting institutions formally acknowledge the asymmetric nature of the relationship they are going to establish and commit to not take advantage, including economic advantage in form of financial profit as stated in Principle 8.

The hosting institution should take into account difficulties, which the sending institution may face if there are language barriers. This includes the process of negotiation, drafting the agreement and preparing different language versions of the final agreement. If the agreement is produced in more than one language, the agreement must also specify which language(s) will be authoritative, as stated in Principle 4.

The relationship between the hosting and sending institutions is one of service: the sending institution specifies the services it requires and the hosting institution agrees to provide them. For example, the hosting institution may state publicly which safe haven services it will provide, but the sending institution will determine which of those it needs.

8. The hosting institution should not financially profit from providing safe haven for specific archives/records. *(No Financial Profit Principle)*

Commentary on Principle 8: No Financial Profit Principle

As a principle, a hosting institution should not receive a financial benefit from providing a safe haven for archives at risk such as by charging high fees for making a copy of a photograph from the deposited materials. If the hosting institution requires all researchers to pay for certain services, such as making copies, the hosting and sending institutions should agree that the institutional charges will apply to the sending institution's materials.

The costs for providing a safe haven solution depend largely on the complexity of the technical solution, the economic situation of the parties and potential external sources for funding. Reliable and sustainable solutions are expensive and providing the necessary infrastructure can be costly. A fee for holding the sending institution's archives/records may be agreed upon between the sending and the hosting institution, but it should not exceed the costs the hosting institution incurs for the technical and infrastructure expenses required to provide the safe haven of the specific archives/records.

Principles on the content of the agreement

9. The agreement shall define the rules and procedures for sending the archives/records, the rules for access to the archives at the hosting institution, its publicity and privacy policies, as well as describe the technical standards, process of storage, preservation and migration of the archives. *(Processes in Agreement Principle)*

Commentary on Principle 9: Processes in Agreement Principle

It is crucial that the agreement between the sending and hosting institution defines the rules and procedures for transferring the archives/records, the rules for access to the archives at the hosting institution, its publicity and privacy policies, as well as describe the technical standards, process of storage, preservation and migration of the archives.

Thus, the agreement or specific annexes to the agreement should specify all technicalities regarding the transfer (protocols for digital archives; means of transfer/transport) and the custody of the archives depending on the material to be secured (paper, digital archives, audio-visual, photo or other) because of different conditions of transfer, preservation, and storage.

10. While the hosting institution becomes the custodian of the archives/records, the sending institution keeps sole ownership, unless otherwise specified in the agreement. *(Ownership Principle)*

Commentary on Principle 10: Ownership Principle

As a rule, the sending institution remains the owner of the secured archives. This implies that it is the sending institution that makes all relevant decisions regarding the description of, access to, destruction and return of the records/archives.

Any deviations from this general rule should be stated clearly in the agreement.

11. When negotiating the terms of the agreement, the parties shall take into account the difficulty of planning the duration of the arrangement and include options for extension and closure. *(Duration Principle)*

Commentary on Principle 11: Duration Principle

In situations of archives at risk, the question of the duration of the agreement and particularly the return of the archives is very sensitive. Further, it is difficult to evaluate to what extent records are still at risk and therefore need still to be secured elsewhere. The agreement needs to strike a balance between the security of the archives and the interests of the sending and the hosting institution. An agreement, therefore, requires a certain degree of flexibility.

The parties should agree on the modalities of the termination of the agreement. Options for the contracting parties include: 1) an agreement with a duration that ends at a specific defined date with the fulfilment of all the contractual obligations of the parties (e.g., the return of the records to the sending institution); 2) an agreement that is extended automatically year by year unless either party gives the other notice of annulment before the end of the contractual period; 3) an agreement for an unlimited period to be dissolved only upon request by one party. Options for ending an agreement by the hosting institution is covered below, in the commentaries on Principle 12.

The agreement should include a clause that allows for immediate termination of the agreement in case of non-compliance, non-execution or breach by one of the parties. Further, if events resulting from *force majeure* (armed conflict or uprisings, natural disaster, et cetera) prevent the execution of an agreement, either of the parties may terminate the agreement from the moment when it becomes impossible to implement it.

12. The sending and the hosting institution must agree on what will happen if either the sending or the hosting institution ceases to exist, or is subjected to major changes in reporting relationships. *(Anticipating Succession Principle)*

Commentary on Principle 12: Anticipating Succession Principle

Archives at risk are usually found where the sending institution is located in fragile contexts. Since such institutions are often under threat themselves, it is not unusual for them to change structures, names, legal status, dissolve, or cease to exist for other reasons. The same can happen to a hosting institution, although it is less likely. Therefore, it is important that the agreement foresees rules regarding succession. Ideally a successor institution takes over the contractual duties of its predecessor as legal successor, although it may be necessary to adapt some contractual provisions. Such changes will need to be negotiated by the remaining and the new contractual party.

If the hosting institution ceases to exist or is no longer in a position to serve as a safe haven, the parties must decide whether and under what conditions the archives/records to be secured will be transferred to another institution. If no transfer to another institution is possible, the person/institution in charge of the liquidation of the hosting institution shall return the materials to the sending institution as defined in the agreement.

In case the sending institution no longer exists, the hosting institution must will negotiate with the successor institution of the sending institution what shall happen to the agreement. If no such institution exists, the hosting institution must make sure that the records are preserved for the sake of the society concerned, in view of potential future use for historical memory, dealing with the past and reconciliation.

In the case of an inter-governmental agreement, in order to protect the agreement even if a change of government occurs in the sending country, the agreement can specify that the hosting will have the right to keep a security copy for a certain period of time or postpone return if returning the archives/records is likely to risk their destruction, their use for repressive purposes, or will place at risk persons whose actions are reflected in the materials.

If the reporting relationship of the hosting institution changes (for example, a national archives is moved from the ministry of culture to the ministry of the interior), the sending institution will be notified and the terms of the agreement may be renegotiated. If the hosting institution is absorbed by another institution, such as a research institute becoming part of a university, the sending institution will also be notified and given the opportunity for renegotiation of the agreement.

13. When interpreting the agreement, the parties shall be guided by the spirit of the moment when the agreement was signed. *(Constituent Spirit Principle)*

Commentary on Principle 13: Constituent Spirit Principle

In case of disagreement between the contracting parties, or in cases where an agreement needs to be amended / interpreted by a successor institution, as outlined above under Principle 12, it is important to go back to the initial purpose and spirit of the agreement for interpretation.

Supporting material such as minutes of meetings, draft versions of an agreement, explanatory notes to the agreement should therefore be kept with the archives for later consultation.

Principles on the Characteristics of Hosting Institutions

14. Hosting institutions should be embedded in an institutional landscape with a functioning, independent judiciary and rule of law, which is likely to prevent inappropriate state influence with the management of the archives/records. They should have support for their activities related to safe haven by their organizational hierarchy and by their governing body. *(Legal Environment Principle)*

Commentary on Principle 14: Legal Environment Principle

In order to guarantee a sure, long-term safe haven solution, it is important that the legal and institutional environment of the hosting institution is stable. This goes for the hosting institution itself, which should be established, have long-term funding, institutional anchorage, a strong legal basis (be it as a foundation or as a public entity) as well as for the political, legal and institutional context surrounding it. A number of indicators can help to assess the stability of the hosting institution and its context. Hosting institutions should be located in areas with no foreseeable internal armed conflict, unrest or occupation from another power.

15. For security and access control purposes, all processing, storage, and preservation facilities and capabilities used to deal with or hold the hosted archives/records should be demonstrably under the direct control of the hosting institution, unless stated differently in the agreement. *(Control of Material Principle)*

Commentary on Principle 15: Control of Material Principle

If any of the facilities of the hosting institution are outsourced or located beyond the physical control of the hosting institution, there should be clear and transparent (e.g., contractual) documentation as to how that direct control is enforced, audited, and assured. There must at least be a service agreement that allows for control. This includes transferring storage of digital information to a cloud service, contracting for audio-visual preservation services, and similar technical support.
If preservation services are outsourced after the conclusion of the agreement, the sending institution needs to be informed and the agreement needs to be amended accordingly.
It is important that any outsourcing solution is in compliance with the agreed international standards.

16. Hosting institutions should have physical characteristics that make them apt to provide a safe haven solution. *(Physical Characteristics Principle)*

Commentary on Principle 16: Physical Characteristics Principle

Ideally, hosting institutions should be located in geographically secure areas with no foreseeable major geological risks (e.g. earthquakes, recurrent flooding). If such risks exist, the hosting institution must show the sending institution that it has taken adequate steps to prevent damage.

17. Hosting Institutions should work in accordance with internationally recognized professional standards. *(Professional Standards Principle)*

Commentary on Principle 17: Professional Standards Principle

The staff members of hosting institutions should have experience or be trained in handling the format to be transferred, in accordance with applicable international standards and for the services required by the agreement. The staff of hosting institutions should further have experience or be trained in handling sensitive, non-public materials.

The hosting institution should provide accountability and transparency with regards to its work.

Storage facilities used for analogue material should comply with recognized national and international standards for records management and metadata management. The storage and preservation capability used for digital material should, when required by the sending institution to achieve their goals, aim to comply with recognised national and international digital preservation standards or certificates.