**Process:** Control of Records

Purpose: To ensure that documented information is available, suitable for use, retained where necessary and adequately protected from damage, loss of confidentiality, improper use or loss of integrity.

Output: Records of evidence of conformity to processes.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S/NO.** | **ACTIVITIES** | **INPUTS** | **RISKS** | **RISK LEVEL** | **RISK IMPACT** | **MITIGATION** | **OPPORTUNITY** | **ACTIONS** |
| 1. | Identification, Distribution and Use | Data, Information and knowledge | * Competence of persons | Medium | High | Assign competent persons for respective tasks | * Use of technology * Adoption of new and best practices in documentation and record management. | * Use technology for records tracking and management. * Technology to facilitate wider accessibility of procedure. |
| * Complexity of process | Create awareness on the procedure |
| * Inadequate information, data | Knowledge and information sharing for records management |
| * Mislabeling of records | capacity building for persons assigned the task |
| 2. | Access, Storage and preservation. | Records of both internal and external origin | * Poor storage facilities i.e cabinets | Medium | High | Provision of adequate storage resources. | * Integration with ISMS Standard for information security * Automation to improve information safety * Benchmarking on new methods | * Establish Archives for retention of records * Use technology to secure soft copy documents |
| * Unauthorized access | Restriction of access by passwords, locks etc |
| * Illegibility | Preservation in the right environment i.e light, humidity |
|  |  |  | * Destruction/ theft/data loss |  |  | * Protection of physical facilities * Provide back-ups |  |
| * Loss of confidentiality/Integrity |  |  | * Administering oath to responsible personnel * Encryption of data * Implement sanctions for reported cases * Sensitization of staff on the procedure for control of records |
| 3. | Retention and Disposition | Evidence of conformity to processes | Unintended alterations | Low | High | * Restriction of access as applicable * Approval and authorization of alterations |  | Develop mechanisms for monitoring the state of records |
| Obliteration of records | Sensitization on procedure |