Classification of information

<The template shall be used for classification of information according to Mid Sweden University's model for information classification. The information classification carried out shall be registered with a confidentiality marking>

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Classification object  Enter the name of the research project. | | | | | | | | | | | | |
| Responsible  Enter the name and title of the person responsible for the information classification.  Participants  Enter the names and titles of the persons who participated in the information classification. | | | | | | | | | | | | |
| Description of information  Describe in point form all amounts of information included in the research. | | | | | | | | | | | | |
| Describe the consequences based on the characteristics:  Describe the impacts and tick the impact level.  Confidentiality:  What will be the consequence if research data leaks to; mass media, other researchers, other countries, the public or staff? What is the biggest damage that can occur? Are any agreements or laws broken if the information is disclosed?  Class 0: No consequences  Class 1: May cause discomfort or limited financial loss to individuals, or limited damage to the University or third parties.  Class 2: May cause significant discomfort or financial loss to individuals, or extensive harm to universities or third-party couples  Class 3: May cause damage to the life or health of individuals, or cause serious discomfort or financial loss to a large number of people, or very serious/catastrophic damage to the University or third parties, based on the University's mission.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Accuracy:  What happens if the information is incorrect? What happens if no one discovers it? What is the worst thing that can happen if the information is incorrect? Can the research results be affected so that the evidence-based recommendations produced on the results are incorrect  Class 0: No consequences  Class 1: May cause discomfort or limited financial loss to individuals, or limited damage to the University or third parties.  Class 2: May cause significant discomfort or financial loss to individuals, or extensive harm to universities or third-party couples  Class 3: May cause damage to the life or health of individuals, or cause serious discomfort or financial loss to a large number of people, or very serious/catastrophic damage to the University or third parties, based on the University's mission.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Availability:  What happens if the information is not available? What will be the consequence if the information is only available to a limited extent or with certain difficulties? Does the accessibility requirement change over different recurring periods and over time? How does it affect progression in  Class 0: No consequences  Class 1: May cause discomfort or limited financial loss to individuals, or limited damage to the University or third parties.  Class 2: May cause significant discomfort or financial loss to individuals, or extensive harm to universities or third-party couples  Class 3: May cause damage to the life or health of individuals, or cause serious discomfort or financial loss to a large number of people, or very serious/catastrophic damage to the University or third parties, based on the University's mission. | | | | | | | | | | | | |
| Confidentiality | | | | Accuracy | | | | Accessibility | | | | CAA value |
| C0 | C1 | C2 | **C3** | A0 | A1 | A2 | **A3** | A0 | A1 | A2 | A3 | Enter the CAA value that the classification has determined. | |
| Safeguards developed (organisational and technical):  Tick the appropriate security measures and complete them if necessary. Organisational and legal aspects: The researchers know what applies to information security at Mid Sweden University and have taken part in the courses available.  A data management plan is in place for the research project.  The project is approved by the Ethical Review Authority.  An agreement has been signed with a data processor and can be found on dnr 20xx/xxxx.  The processing contains personal data and is listed in accordance with Article 30 of the GDPR.  The processing requires an consequence assessment according to Article 35 GDPR and one is carried out. Technical Security measures that provide adequate protection of research data when the University's common IT services are used by the research project: Storage : High protection value documents are stored on MIUN internal workspaces or in the Vault (Confidentiality=2,3, Accuracy=2,3).  Documents with protection value Confidentiality = 0- 1, Acccuracy = 0-1 can be stored in M365 services or on local or external hard drive, USB/plate/memory card unencrypted.  Physical documents are kept in approved lockers and premises.  Access and access:  The principal investigator assigns, approves, checks access rights to the research data of the project.  User accounts:  The MIUN joint login service is used.  The account is protected so that it does not get into the wrong hands with the help of strong authentication, multi-factor authentication (MFA), whenever possible.  Workstation:  Computers must have an appropriate level of protection.  Automatic security updates for operating systems, applications and tools are turned on to reduce the risk of vulnerabilities being exploited to access protected information or account details.  Antivirus software that notifies deviations is used.  The computer firewall is activated.  VPN  Used when working outside the university to get a protected communication between computer and Mid Sweden University.  Backup/backup  Research data and analysis results are backed up.  Information stored on MIUN's internal workspaces and in the Vault is backed up.  Encryption  When files with a high protection value are sent by email, encryption is used.  To protect information in case of theft, your computer's hard drive is encrypted.  Other security measures  The code key for pseudonymisation is kept separate from the source data.  Physical protection  Premises where data media are stored are protected by a perimeter protection (locks, alarms, access systems, etc.).  When equipment is moved between users within the department, or is to be discarded, replaced or sold, Mid Sweden University's procedures for handling discontinued IT equipment must be followed.  Incidents  If an IT security incident or personal data breach occurs, it is reported promptly to ITsupport@miun.se.  Travelling  There is an awareness of guidelines for mobile equipment and what applies when handling equipment during travel.  Data – life-cycle management  There is a plan for storage, thinning, archiving and possible decommissioning. | | | | | | | | | | | | |