Information Risk Classifications

Information is vital to the University's mission. We are committed to protecting its confidentiality, integrity and availability, and the privacy of students, staff and alumni and all individuals we work with.

The University of Glasgow classifies its information assets into risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorised access.

Risk Classifications

Low Risk	Medium Risk	High Risk
Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk, and: 1 The data is intended for public disclosure, or: 2 The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.	Data and systems are classified as Moderate Risk if they are not considered to be High Risk, and: 1 The data are not generally available to the public, or: 2 Defined by the GDPR as "personal data", or: 3 The loss of confidentiality, integrity, or availability could have a mildly adverse impact on our mission, safety, finances, or reputation.	Data and systems are classified as High Risk if: 1 Defined by the GDPR as "special category data" see list directly below, or: 2 The loss of confidentiality, integrity, or availability could have a significant adverse impact on our mission, safety, finances, or reputation, or result in damage/distress to students, staff or other individuals.

Information/Data Risk Classification Examples

Use the examples below to determine which risk classification is appropriate for a particular type of data

When mixed data falls into multiple risk categories, use the highest

Low Risk	Medium Risk	High Risk
▪ Research data (at PI discretion) ▪ Staff work contact info ▪ Policies and Guidance, unless specific requirement to restrict ▪ College/School/Course details, marketing or press Information ▪ Job adverts ▪ Publicly available campus maps ▪ Anything in UofG FoI publication scheme ▪ Information in the public domain	▪ Unpublished research data (at PI discretion) ▪ Student names and email addresses ▪ Individuals' dates of birth, personal contact details (e.g. home address, phone number) ▪ NI or passport numbers ▪ Staff and student ID numbers ▪ Unpublished planning and budgeting info ▪ Commercially sensitive information ▪ Embargoed theses	▪ Special Category data - personal data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a person, health, sex life or sexual orientation ▪ Criminal convictions or alleged offences ▪ Individuals' financial information, including credit card/bank numbers. ▪ **Details of many individuals, that would otherwise be rated Medium Risk.*** ▪ Donor contact information and non-public gift information ▪ Exam questions prior to use

*****For specific questions on "details of many individuals" and the risk level contact dp@gla.ac.uk

For advice on medium and high-risk data management read the Confidential Data policy.

Application Risk Classification Examples

An application is defined as software running on a server that is network accessible

Low Risk	Medium Risk	High Risk
• Applications handling Low Risk data • Online Maps • Online catalogue displaying academic course descriptions	• Applications handling Medium Risk data	• Applications handling High Risk data • HR application that stores staff bank details • Application collecting personal information of donor or alumni. • Application that processes credit card payments.

Server Risk Classification Examples

A server is defined as a host that provides a network accessible service.

Low Risk	Medium Risk	High Risk
▪ Servers used for research computing purposes without involving Moderate or High Risk data. ▪ Servers used to store published public data.	▪ Servers handling Medium Risk data	▪ Servers handling High Risk data ▪ Servers controlling access to other systems ▪ Email servers ▪ DNS and DHCP servers ▪ Active Directory servers

Authors: Chris Edwards, Diane Montgomery, IT Services
Johanna King, Head of DP/FoI Office
V 1.03 01.02.18

Draft update for GDPR