# Data Classification Guide

## Purpose and Scope

1. Define the classification of data assets, the default classification of information.
2. This classification applies to all information created or received by the Company in the course of official business, whether in physical or digital form. This includes paper documents, electronic files, drawings, maps, plans, photographs, microfilms, audio/video recordings, database records etc.

## Data Classification Frameworks

1. The Security Classification Framework (SCF), classifies data based on (a) potential damage to the Company; and (b) the potential damage to public health and safety, if the data is disclosed without authorization; and
2. The External Sensitivity Framework (ESF) which classifies data based on the potential impact to an individual or entity if the data is disclosed without authorization.

## SCF Framework

The SCF framework establishes guidelines for data security classification based on assessing the potential consequences of unauthorized disclosure to public health and safety and/or the Company image and interests[[1]](#footnote-1). The classification levels can be found in Table 1:

Table 1: Classification Levels under SCF Framework

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Information which will not negatively affect public health and safety or the Company’s image and interests if disclosed without authorization, shall be either: | | Information which will negative affect public health and safety or the Company’s image and interests if disclosed without authorization, shall be: | | | | | |
| Class Light Green | Class Dark Green | Class Blue | Class Yellow (NA) | Class Yellow (NB) | Class Orange | Class Red | Class Black |
| Suitable and useful[[2]](#footnote-2) to be publicly disclosed. | Unsuitable or not useful to be publicly disclosed. | Some damage to the Company and our partners[[3]](#footnote-3). | Some damage to public health and safety[[4]](#footnote-4), or serious damage to the Company. | Serious damage to the Company[[5]](#footnote-5) with no damage to public health and safety. | Serious damage to public health and safety, or exceptionally grave damage to the Company. | Exceptionally grave damage to public health and safety. | Global catastrophe and societal collapse. |

Refer to Table 2 for examples illustrating the degree of damage to the Company and/or public health and safety under the various classification levels.

Table 2: Degree of damage to the Company and/or public health and safety

|  |  |  |
| --- | --- | --- |
| Key Classifications | Public Health and Safety | Company’s Interests |
| Class Black  *Global catastrophe and societal collapse.* | <redacted> | N/A |
| Class Red  *Exceptionally grave damage to public health and safety.* | * National containment plans * Information relating to internal security operations and plans vital to protecting public health and safety. | N/A |
| Class Orange  *Serious damage to public health and safety, or exceptionally grave damage to the Company.* | * Widespread loss of lives or extensive public disorder | * Impediment of critical processes of the Company, resulting in its inability to uphold public health and safety * Serious disruption to services essential for public health and safety or maintenance of public order * Serious disadvantages in negotiations affecting public interests or the Company * Serious disruption to the financial or economic system of the country |
| Class Yellow  Some damage to public health and safety, or serious damage to the Company | * Limited public disorder | * Some disruption to services essential for public health and safety or maintenance of public order * Some disadvantages in negotiations affecting public interests or the Company * Some disruption to the financial or economic system of the country * Impediment of the Company’s critical processes resulting in its inability to discharge its functions (i.e. Class Yellow (NB)) |
| Class Blue  Some damage to the Company | N/A | Impediment of the Company’s processes resulting in hindrance to discharge its functions |

## ESF Framework

While the SCF Framework protects classified information, the ESF Framework specifically addresses the sensitivity classification of data relating to individuals and/or entities (excluding the Company). It evaluates how unauthorized disclosure could affect individuals or entities. The classification levels can be found in Table 3:

Table 3: Classification Levels under ESF Framework

|  |  |  |
| --- | --- | --- |
| S1 | S2 | S3 |
| Information whose unauthorized disclosure poses no risk of physical, financial, or emotional damage to the individuals or entities. This typically includes personal or organisational information that is generally considered public knowledge. | Information whose unauthorized disclosure causes temporary minor emotional distress or discomfort to individuals (e.g. from disclosure of images or location data), or reduction in competitive advantage or compromised business interests of entities. | Information whose unauthorized disclosure of information causes severe physical, financial damage, prolonged[[6]](#footnote-6) emotional trauma or social stigmatisation to individuals (e.g. threats to life, loss of life or physical harm, loss of employability), or sustained financial losses, significant disruption of normal operations or permanent damage to competitive advantage of entities. |
| Examples of such information are hashed Customer Account Numbers or national identification numbers that cannot reasonably be re-identified, employee ID numbers, and numbers that have limited use outside of the Company, test data that contains mock or masked records of individuals, publicly disclosed contact information on publicly available websites. | Examples of such information are Customer Account Numbers in full or masked but vulnerable to reconstruction, national identification numbers in full or masked but vulnerable to reconstruction, address[[7]](#footnote-7) or staff training and development plans. | Examples of such information are case information revealing the identity of victims of serious crimes; criminal or investigation records for serious crimes; identity of participants in sensitive test trials; identity of customers with sensitive medical records; or trade secrets of an entity. |

If the information is not enough to identify any individual or entity (excluding the Company), the classification is ‘S1’.

The ESF Framework’s sensitivity assessment excludes potential impacts of unauthorized disclosure to us (i.e., the Company) as these are already covered under the SCF Framework. Therefore information about the Company should be classified as ‘S1’ under ESF as long as there are no impacts to individuals or entities.

When determining data sensitivity, teams must evaluate the direct and reasonably foreseeable consequences that unauthorised disclosure would have on the affected individual or entity. A direct impact is one that follows immediately from the disclosure itself, rather than impacts that might occur only if combined with other circumstances or events. The assessment should focus on consequences that are certain, likely, or probable, rather than those that are unlikely or rare occurrences.

Teams must conduct a new assessment of both security and sensitivity classifications whenever data undergoes changes in its format or level of detail, ensuring that the classifications remain appropriate and accurate.

## Default Classification

Our data assets can be split into four categories, each of which shall be applied with default classification for data items within each category.

1. Policy, Experimental and Research Records;
2. Corporate Records (Personnel);
3. Corporate Records (non-Personnel);
4. Customer and test subject Records

Teams are to use the default classifications below as a guide.

Table 4: Policy, Experimental and Research Records

|  |  |
| --- | --- |
| **Category** | **Classification** |
| * Policy, experimental and research records shared with the Leadership Core (i.e., the Executive Council, Chairman, President and/or Founder), decisions by the Leadership Core, and notes by any one of the Leadership Core where unauthorized disclosure results in serious damage to public health, safety and/or trust * Data and information from sensitive experiments and research that can cause widespread distrust and hostile actions by the public against the Company | Class Orange / S1 |
| * Reviews and studies that are shared with our shareholders * Inputs to policy documents, experimental approaches and research directions * All other policy, experimental and research records shared with the Leadership Core, decisions by the Leadership Core, and notes by any one of the Leadership Core that are excluded from Class Orange and above. | Class Yellow / S1 |
| * Reviews and studies that are internal to the Company * Non-public experimental and research pieces | Class Blue / S1 |
| * Corporate policies e.g. Code of Conduct, Financial Regulations etc. * Approved work processes/ SOPs/ operational guidelines/ team policies | Class Dark Green / S1 |
| Other policy, experimental and research records | Class Blue / S1 |

Table 5: Corporate Records (Personnel)

|  |  |
| --- | --- |
| Category | Classification |
| * Involvement in sensitive projects and research | Class Orange / S1 |
| * Disciplinary records * Investigation records * Criminal records * Sensitive medical conditions, such as terminal illnesses, sexually transmitted diseases, disabilities etc. | Class Blue[[8]](#footnote-8) / S3 |
| * Sensitive records for personnel who are leaving or have left the Company, such as poor conduct/ performance, disciplinary issues | Class Dark Green / S3 |
| * Administrative Records * Claims * Leave * Awards * Scholarships * Training * Appointments * Training evaluation/feedback * Personality reports | Class Dark Green / S1 |
| * Employee financial and non-financial statuses * All other medical conditions * Salaries, performance bonuses, other pay-outs, benefits, allowances, increments, salary adjustments, bank account details) * Terms and conditions of employment (security clearances, pay grade, job grade) * Performance appraisal records, competency evaluations * Internal survey responses from staff | Class Blue[[9]](#footnote-9) / S2 |
| * Personal details of employees (e.g., name, personal identification number, address, date of birth, family details, marital status, race, religion, nationality, education, employment records etc.) * Recruitment details (e.g., interview details, interviewer’s comments etc.) * Exit details (e.g., Date of resignation, notice period etc.) | Class Dark Green / S2 |
| * Bankruptcy records * Team within the Company * Job title * Staff business contact information | Class Light Green / S1 |
| * Other Corporate (Personnel) Records | Class Blue[[10]](#footnote-10) / S2 |

Table 6: Corporate Records (Non-Personnel)

|  |  |
| --- | --- |
| Category | Classification |
| * Information about sensitive projects and research | Class Orange |
| * Information related to cybersecurity defences | Class Yellow (NA) / S1 |
| * Physical safety and security-related information and records | Class Yellow (NB) / S1 |
| * Minutes and materials of key meetings (e.g. includes the Leadership Core, other companies’ leadership etc.) * Financial and accounting records and transactions * Procurement records (before publishing) * Contractual records and agreements with other companies and the government * Audit records | Class Blue / S1 |
| * Staff activities * Internal committee meetings * Media campaigns (before release) * Training materials * Office supplies records * Building management / maintenance / operations * Off-the-shelf system documentation and materials, excluding higher classifications | Class Dark Green / S1 |
| Other corporate (Non-personnel) records | Class Blue / S1 |

Table 7: Customer and Test Subject Records

|  |  |
| --- | --- |
| **Category** | **Classification** |
| * All personal details of test subjects involved in sensitive projects or research | Class Orange |
| * All personal details of test subjects in non-sensitive projects or research | Class Yellow (NA) / S2 |
| * Customer sensitive medical records (e.g. sexually transmitted diseases, serious mental illnesses, addictions, terminal illnesses, disabilities, transplants, suicide or attempted suicide, abortion, abuse etc.) * Customer next-of-kin details | Class Blue[[11]](#footnote-11) / S3 |
| * Personal information of customers * Account balances of customers * Account transactions of customers * Salary details of customers * Employer information of customers * All other medical records not covered under a higher classification | Class Blue[[12]](#footnote-12) / S2 |
| * Public interactions with customers (e.g., emails, physical visits, appointments, calls, etc.) | Class Dark Green |
| Other customer records | Class Blue / S2 |

Approval for Data Reclassification

Reclassification can only be done through approval from at least one of the Leadership Core, with inputs from the Data Classification Committee. Teams must maintain proper documentation of the approval and submit all relevant documents to the Data Classification Committee.

Reclassifications to Class Light Green cannot be reversed.

1. Damage to reputation or embarrassment of the Company is generally not a primary consideration when assessing data security classification. However, if reputational damage directly impacts the Company or public health and safety (i.e. the Company’s ability to function), it can be taken into account when assessing data security classification. [↑](#footnote-ref-1)
2. Employees shall assess usefulness of sharing data to the public based on demand from the public, potential benefits to the public (e.g. commercial, academic, or research value), or potential benefits to achieving the Company’s objectives. Do note that the sharing should not be made if it is not practical, prohibited by law or control, or compromises public trust and confidence in the Company’s management and protection of data. [↑](#footnote-ref-2)
3. Unauthorized disclosure of information would likely cause a disruption to the Company’s process resulting in a hindrance to discharge its functions. [↑](#footnote-ref-3)
4. Matters of concern of importance to society, in public health and safety. Please note that the listed examples are not exhaustive. [↑](#footnote-ref-4)
5. Unauthorized disclosure of information would likely cause a disruption to the Company’s critical process resulting in its inability to discharge its functions, but should not cause damage to public interests (e.g. Classified staff training information, closed procurement records dataset). Beyond the changes in hosting requirements for Class Yellow (NB) systems, there will be no changes to security requirements for such systems and documents (i.e. these systems have the same security requirements as Class Yellow (NA). [↑](#footnote-ref-5)
6. Sustained injury or stigma occurs when the individual generally has no modes of recourse or alternatives to remedy outcome of unauthorized disclosure. [↑](#footnote-ref-6)
7. Address is classified as ‘S2’ only if we can identify whom the address belongs to. For example, if the dataset contains only the address and there is no other easily accessible dataset to compare against, the address would be ‘S1’ since we cannot identify to whom it belongs to. [↑](#footnote-ref-7)
8. Unless the record contains only 1 person, in which case it will be classified as Class Dark Green [↑](#footnote-ref-8)
9. Unless the record contains only 1 person, in which case it will be classified as Class Dark Green [↑](#footnote-ref-9)
10. Unless the record contains only 1 person, in which case it will be classified as Class Dark Green [↑](#footnote-ref-10)
11. Unless the record contains only 1 person, in which case it will be classified as Class Dark Green [↑](#footnote-ref-11)
12. Unless the record contains only 1 person, in which case it will be classified as Class Dark Green [↑](#footnote-ref-12)