

## Example Information Classification Rules & Level

### Confidential

- I. Any financial account number e.g., depository, savings, debit and credit card accounts, investment advisory or brokerage accounts, loans).
- II. Employment history e.g., resumes, prior jobs, prior employers, current job tenure).
- III. Financial Transaction e.g. payee and payor information with or without account number or debit/credit amounts).
- IV. Small business Tax Code.
- V. Any Social Security Number
- VI. Any Passport information
- VII. Payment Number (Check)
- VIII. Veterans Preference
- IX. Highly sensitive data that will explicitly identify individuals which, if disclosed, puts the individual at risk from identity theft, social or legal sanctions, targeting by marketing corporations or pressure groups, threats from criminal or vigilante individuals or organizations
- X. Any data which is classified Credit report data e.g personal, financial details
- XI. Financial Transaction e.g. Procurement Card Number , Procurement Card number
- XII. Financial information regarding individuals e.g. payment information (credit card details), bank account details, information about indebtedness (student fees).
- XIII. Draft research reports of controversial and/or financially significant subjects
- XIV. Preliminary degree classification or transcript information pending formal approval and any publication
- XV. Driver license
- XVI. Any data which is classified as Health related data e.g Health Care number, Health care Province
- XVII. Any data which is classified as Military related data e.g Military Grade, Military Status
- XVIII. Future marketing or student fees information not yet agreed to be made public.

### Restricted

- I. Self-selected shared secret for authentication credential.
- II. Private key of an asymmetric cryptographic key pair.
- III. Secure One Time Authentication (SOTA).
- IV. Secure token authentication information (i.e., applies to the combined data elements of PIN and token value).
- V. Passwords
- VI. Care Verification Value
- VII. Personal ID number (PIN)
- VIII. Passphrase
- IX. Biometrics e.g, voice, palm, fingerprints, iris, face scan
- X. Private key of an asymmetric cryptographic key pair
- XI. Symmetric encryption

- XII. Personal data identified under the Data Protection Act 1998 (or its successor legislation). For more information on GDPR within the University please visit:
- XIII. Internal correspondence, timesheets, expenses.
- XIV. Exam scripts, exam marks, examiner's comments on a student's performance
- XV. Incomplete reports and other documents whose integrity may be damaged by uncontrolled/ unauthorized changes, or whose leakage may cause damage to the project, the project funders or the Institute

## **Internal**

- I. Credit Card cash rewards balance; cash rewards earned this period e.g, cash back earned, or cash back paid to a specific customer over a specified time period.
- II. Employee education history/learning transcript Info e.g., courses taken, assessment scores, dates).
- III. General job demographics e.g., title, dept, manager, work city, market value estimate
- IV. Passwords that protect document formatting and internal use information.
- V. General University data: all staff internal memoranda
- VI. University policy and procedures
- VII. Unauthorized disclosure or destruction of internal use information could have minimal impact to consumers, Organization, its customers, or employees
- VIII. Data that is already in the public domain but was not intended as such and could result in litigation if republished.
- IX. Staff directory including email addresses.
- X. Internal use information is generally shareable between employees with a basic need-to-know e.g, Post Amount , post base amount , highest pay plan
- XI. Salary related information e.g, salary administration plan, highest grade
- XII. salary grade

## **Public**

- I. Data obtained through public source as long as the data excludes non-public personal information.
- II. Data obtained through public source as long as the data is not associated with an individual current or former employee, contractor or applicant.
- III. Anonymous data.
- IV. Title
- V. Public data will have no significant impact if they are altered or viewed in an uncontrolled fashion.
- VI. Disclosure of public information, by itself, would not result in harm to consumers, Organization, its customers, or employees.
- VII. Principal University contacts e.g. name/email address/telephone numbers for public-facing roles will be made freely available

- VIII. Public information refers to information either commonly available openly in the public domain or intended for unrestricted use beyond organization.
- IX. Annual account
- X. Program and course information
- XI. Personnel status
- XII. Telephone
- XIII. Remit details e.g, remit vendor , remit to location, remitting address, ordering address
- XIV. Geo code other details