RED Security Policy & Procedure

People, Assets & Information

RED

2024

☐ PUBLIC ■ INTERNAL ☐ RESTRICTED ☐ SECRET

A company of TRACTEBEL ENGIE

REVISIONS

Status	Date	Created / Updated By	Purpose	Revision Details	Approved by
1	24 October 2023	Shereen Torry	New Document	New Document. Developed in accordance with ENGIE's Group Security Procedure	Mark Smith
2.	22 April 2024	Shereen Torry	Update	Information security updates	Paul Wilson, Michael Rodrigues
3.	05/12/2024	Shereen Torry	Update	Information security updates	Paul Wilson, Michael Rodrigues

DOCUMENT STATEMENT

Purpose

This document is dedicated to the protection of RED's People, Assets and Information against malicious acts to always make our operations and investments possible, in all places and under all circumstances.

It aligns with ENGIE Group's People and Property Security Policy in terms of organisation and missions in the fields of security and business intelligence.

It is the responsibility of leadership to implement this Policy in all locations within RED.

Scope

This document was validated by Chief Operating Officer and applies to all employees within the Company. It also applies to third parties (contractors, sub-consultant) handling RED data and/or with access to RED's physical assets and facilities.

Responsibilities

The Chief Operating Officer shall be responsible for approval and oversight of this document which shall be periodically reviewed by Head of Health, Safety & Security and Head of Information Security and the Data Governance Committee with material changes reviewed and approved by the Chief Operating Officer in accordance with internal requirements, ENGIE's mandated policies, regulation or other guidance change.

All employees are responsible for implementing procedures outlined within.

Training & Communication

All employees shall receive training on their respective role and expected actions. This document is communicated through RED's Resource Site (SharePoint) Document Library.

The mandatory requirements set out within will be communicated to new employees through training and as part of the company's onboarding process.

Refresher training will be provided to all employees as changes occur and communicated out on the company's SharePoint site accordingly.

Change Control and Review

This document should be reviewed on an annual basis or revised with changes. Updates will be managed in accordance with the Quality Management System's document control Procedure.

Compliance

Compliance and effectiveness of this Procedure will be monitored through various methods, including but not limited to business tool reports, internal and external audits, and feedback.

Exceptions

Any exceptions must be approved by the Data Governance Committee in advance.

Non-Compliance

Incidents of non-compliance will be handled in accordance with the Company code of conduct and disciplinary Procedure if applicable.

The following icons are used throughout the Policy to indicate supporting resources as follows:


Relevant SharePoint Areas


Relevant Mandatory Training


Relevant Contacts

CONTENTS

RED

2024

RED SECURITY POLICY

RED's Security Policy is applicable to all employees and is required to ensure

- the protection of all people associated with our activities wherever they operate
- the protection of RED's workplace locations
- the protection of RED's assets – computer and other devices, servers and other innovation assets
- the protection of data – keeping client and project data safe and secure and ensuring appropriate transmittal of data plays a crucial part in ensuring we meet our contractual obligations with them

THE POLICY IS ORGANISED INTO THREE CORE AREAS

PEOPLE SECURITY

Security associated with people

Protection of people at work and on international business trips.

ASSET PROTECTION

Security associated with critical infrastructures and assets

Protection of physical and digital assets covering two categories of assets (1)office & workplace facilities and (2)company equipment and devices.

INFORMATION SECURITY

Security associated with sensitive information

Protection of data, information and information system.

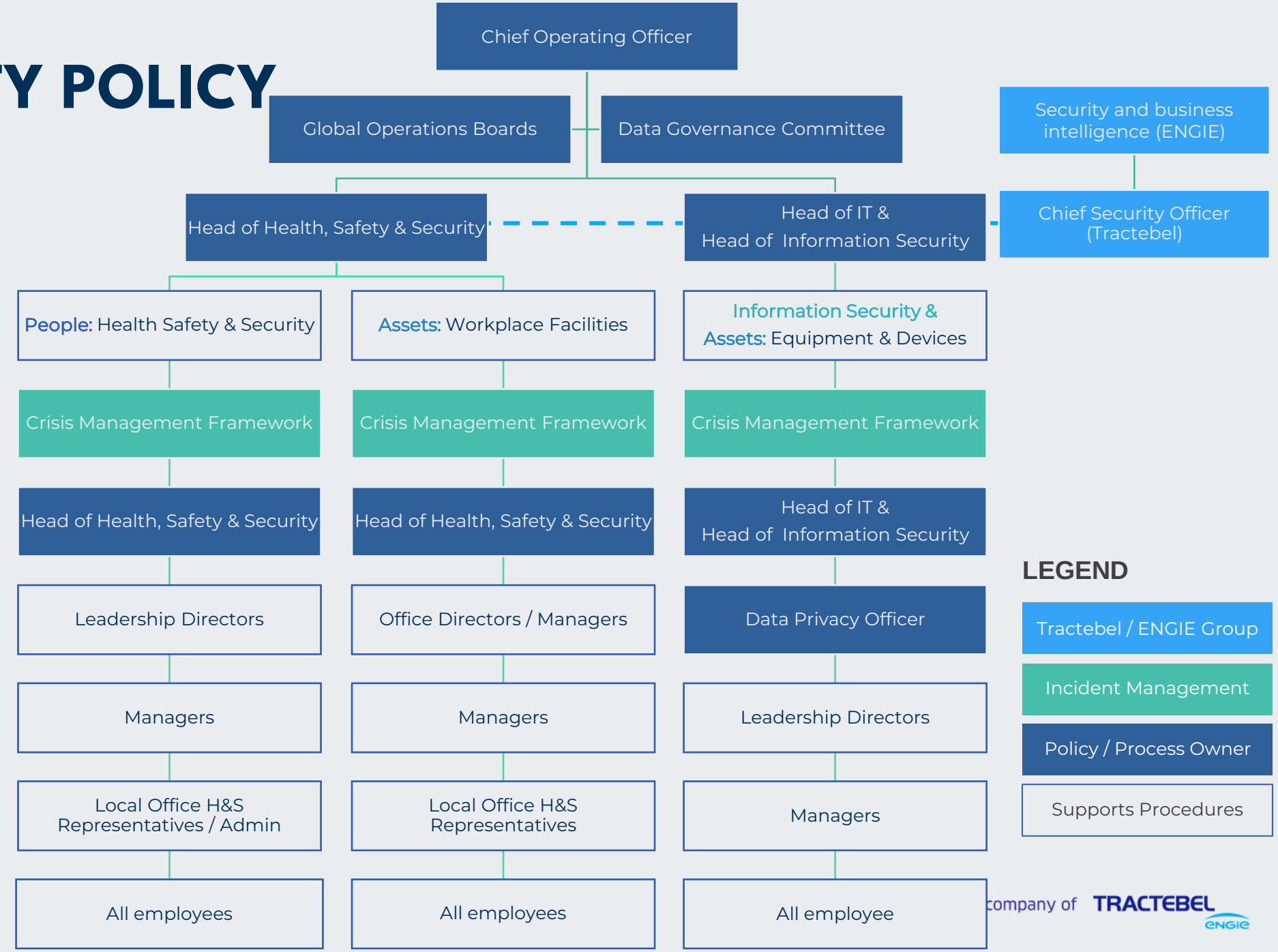
REMINDER: Security is **everyone's** responsibility - employees should always keep security top of mind!

RED SECURITY POLICY

Roles & Responsibilities

The structure on the right outlines responsibilities and reporting lines associated with the implementation of this policy across the three core areas of People, Assets and Information.

Where security incidents occur, these are managed through the incident management procedure supporting RED's Crisis Management Framework.



RED

2024

company of TRACTEBEL ENGIE

Security of People

RED SECURITY POLICY: PEOPLE SECURITY

Protecting the lives of all those who work for us is at the heart of what we do as a socially responsible company.

Below outlines the policies and procedures we have in place to support People Security.

Security of people on international business trips

All international travel must be arranged through a member of the admin team to ensure compliance with RED Travel Policy.

ISOS is RED's travel risk management partner and forms part of the Travel Policy. All travellers are required to download the ISOS Assistance App and complete ISOS Training Modules.

Security of people at work (workplace)

Local Office Quick Sheet outline health, safety and security guidance along with dos and don'ts for each office.

RED's office related H&S Procedure include:

- ✓ Ergonomics assessment
- ✓ Personal Emergency Egress Plan (PEEP) Evacuation Assessment
- ✓ H&S Equipment Request Form
- ✓ Desk booking on Living@
- ✓ Office risk assessment and mitigation measures
- ✓ Control of substance hazardous to health and provision of safety data sheets
- ✓ Manual Handling assessment and training where required

Security of people at work (site)

Employees are expected to understand and follow

- ✓ ENGIE's 9 Life Saving Rules
- ✓ ENGIE's Safety Essentials

RED's site related H&S Procedures include:

- ✓ Client/Site Meeting Procedure
- ✓ Risk Assessments & Method Statements
- ✓ Personal Protective Equipment Policy & Guidance
- ✓ H&S Equipment Request Form (includes PPE)
- ✓ Site/Client booking on Living@
- ✓ Employee & Contractor Induction
- ✓ Resident Engineer Reporting
- ✓ Client contractual & local legal requirements

People Security Resources

Health, Safety & Security

RED QHSSE Induction
ENGIE One Safety Induction
IHASCO e-Learning modules
ISOS Travel Risk Modules

Local Office Representatives

RED

2024

A company of TRACTEBEL ENGIE

Security of Assets

RED SECURITY POLICY: ASSET PROTECTION

Asset protection is the protection of physical and digital assets from unauthorised access, use, disclosure, disruption, modification or destruction.
It covers measures designed to deny unauthorised access to RED's office facilities as well keeping company equipment and devices safe and secure.

Asset controls in place

Offices & Workplace Facilities

Most of our offices benefit from having:

- ✓ CCTV surveillance
- ✓ Security guards
- ✓ Protective barriers / Locks
- ✓ Access control
- ✓ Perimeter intrusion detection,
- ✓ Deterrent systems
- ✓ Fire protection, and other systems designed to protect persons and property.

Company Assets

- ✓ ENGIE INTUNE (Office 365)
- ✓ Tractebel Digital Identity Policy

Employee are expected to keep the workplace secure

- ✓ NEVER share your access code, card or keys
- ✓ NEVER hold secure doors open for anyone who doesn't have a badge
- ✓ ALWAYS protect and secure your access badge/keys
- ✓ ALWAYS restrict unauthorised Visitors
- ✓ ALWAYS report suspicious Behaviour
- ✓ NEVER tamper with secure systems & controls
- ✓ Know Your Access Privileges
- ✓ ALWAYS follow instructions from Management & Security

Employees are expected to keep company assets secure

- ✓ ALWAYS keep your company asset(s) safe and secure
- ✓ ALWAYS lock your computer when leaving the area
- ✓ ALWAYS keep your password confidential and change it regularly
- ✓ ALWAYS secure valuables
- ✓ NEVER Leave your company devices unattended when outside of company premises
- ✓ NEVER share your password, write it down or use the same password across multiple platforms
- ✓ NEVER leave your device unlocked and unattended

Asset Security Protection

Health & Safety
IT & Infosec

RED QHSSE Induction
RED IT Induction
IHASCO e-Learning modules
ISOS Travel Risk Modules

Local Office Representatives

A company of TRACTEBEL ENGIE

Security of Information

RED

2024

A company of TRACTEBEL ENGIE

RED SECURITY POLICY: INFORMATION SECURITY

Information security is the protection of data, information and information system.

TYPES OF DATA / INFORMATION

Client / Project Data

RED's Project Data Management Handbook outlines the expectations of employees handling client and project data.

RED has contractual obligations with clients around the location/security of their data. These obligations vary depending on the client.

Any loss or breach of data obligations must be reported to the client in accordance with agreements in place with them.

Therefore, it is imperative that any specific limitations are clearly understood by employees. Refer to your team Project Manager / Director for guidance on specifics associated with the client / project data you are handling.

Personal Data

Personal data means any information relating to an identified or identifiable person.

RED's Data Privacy Framework explains RED's personal data protection practices

In the wrong hands, personal data could put the data subject at serious risk. To protect individuals, sensitive personal data must be treated with an elevated level of awareness and security in accordance with the above Framework.

RED has legal and regulatory obligations around the protection of personal data and are required to report any breaches to the Information Commissioners Office (ICO) within 72 hours.

Sensitive Business Data

Sensitive business data is information, that, if exposed could cause threat to the company's reputation, operations or competitive edge (i.e. financial data, intellectual property, business strategies, legal agreements/contracts, operational information, internal policies/procedures.

Employees must take extra care when storing such information and consider the appropriate restricted area as guided by the Department Head.

It is of paramount importance, to ensure that no sensitive business data is shared with anyone who isn't deemed appropriate by association and/or without approval from the relevant Department Head.

Information Security Protection

Legal - Data Privacy
IT / information Security

Data Protection
Cyber Security

Data Privacy
Information Security

RED SECURITY POLICY: INFORMATION SECURITY

Information security is the protection of data, information and information system.

INFORMATION SECURITY PROTOCOLS

Employees

Everyone has a part to play in the security of information and data.

Employees are expected to keep company information secure and to comply with the company's Information Security Dos & Don'ts.

Office Information Security Protocols

- ✓ Confidential waste is provided in each office
- ✓ Confidential lockers and/or cupboards are available in each office with restricted access
- ✓ All restricted IT areas (containing critical IT resources) shall be restricted and have auditable access controls in place based upon roles and responsibilities
- ✓ All physical network points are secure to 802.1X security standard or disabled if inactive
- ✓ IT follow ENGIE Backbone Rules and ensure any vendors / authorised visitors are escorted in server rooms at all times
- ✓ IT require authorisation before disposing, relocating, or transferring hardware, software, or data to any offsite premises.

Asset controls in place

- ✓ Project Data Management Handbook
  - ✓ Data Storage
  - ✓ M365 Environment
  - ✓ Use of Other EDMS
  - ✓ File Transfers
  - ✓ Access Control ENGIE Cyber Security Policy
- ✓ Data Privacy Framework
- ✓ Information Security Policy
- ✓ ENGIE Email Security Standard
- ✓ Tractebel Digital Identity

Information Security Protection

Legal - Data Privacy
IT / information Security

Data Protection
Cyber Security

Data Privacy
Information Security

RED

2024

A company of TRACTEBEL ENGIE

RED SECURITY POLICY: INFORMATION SECURITY

Employees are expected comply with the company's Information Security Dos & Don'ts.

DO

ALWAYS keep company asset(s) safe and secure.	ALWAYS lock device(s) when away from your desk in the workplace.	ALWAYS ensure your company device(s) are up to date with company security updates.	ALWAYS log out after any online sessions.
ALWAYS keep your password confidential and change it regularly.	ALWAYS be suspicious of emails from people you do not know.	ALWAYS be cautious of emails that ask you to enable macros to view content.	Avoid sharing attachments in emails – use links to allow for access management.
ALWAYS use encryption when emailing sensitive information.	ALWAYS double check recipient eacmail addresses before sending emails.	Separate personal and professional use. Use your personal device for personal and company device for professional use.	ALWAYS comply with Policy and follow guidance. Report incidents immediately.

DO NOT

Leave your device(s) unlocked when unattended in the workplace.	Leave your company device(s) unattended when outside of company premises.	Store any employee, customer or project data locally on your laptop, tablet or mobile phone.	Download any employee, customer or project data to an external storage device.
Share/transfer personal data outside of the company unless compliant with RED's Data Privacy Policy.	Share your password, write it down or use the same password across multiple platforms.	Click on links or download attachments contained in suspicious emails.	Use a personal device for professional use.

Appendices

RED SECURITY POLICY: CLASSIFICATION OF INFORMATION

Emails & Microsoft Office documents – restrictions & protections automatically applied based on the selected classification level (using the “Sensitivity” button in Outlook, Word, Excel and PowerPoint):

Application	Label Name	Data Level (Office Document / Email)			Container Lever (Teams/SharePoint)			Comments
		Encryption	Protection	Permissions	Privacy	External User Access (Teams)	External Sharing	
Outlook	Non-Confidential	☒	☒	N/A				
	Confidential	☑	☑	User defined (email recipients)				Recipients have all usage rights except save as, export and full control. This means they have no restriction (they can forward the email, print or copy from it) but cannot remove the protection. Unprotected office documents attached inherit this protection.
	Strictly Confidential	☑	☑	User defined (email recipients)				Recipients cannot forward the email, print or copy from it. Unprotected office documents inherit the same protection.

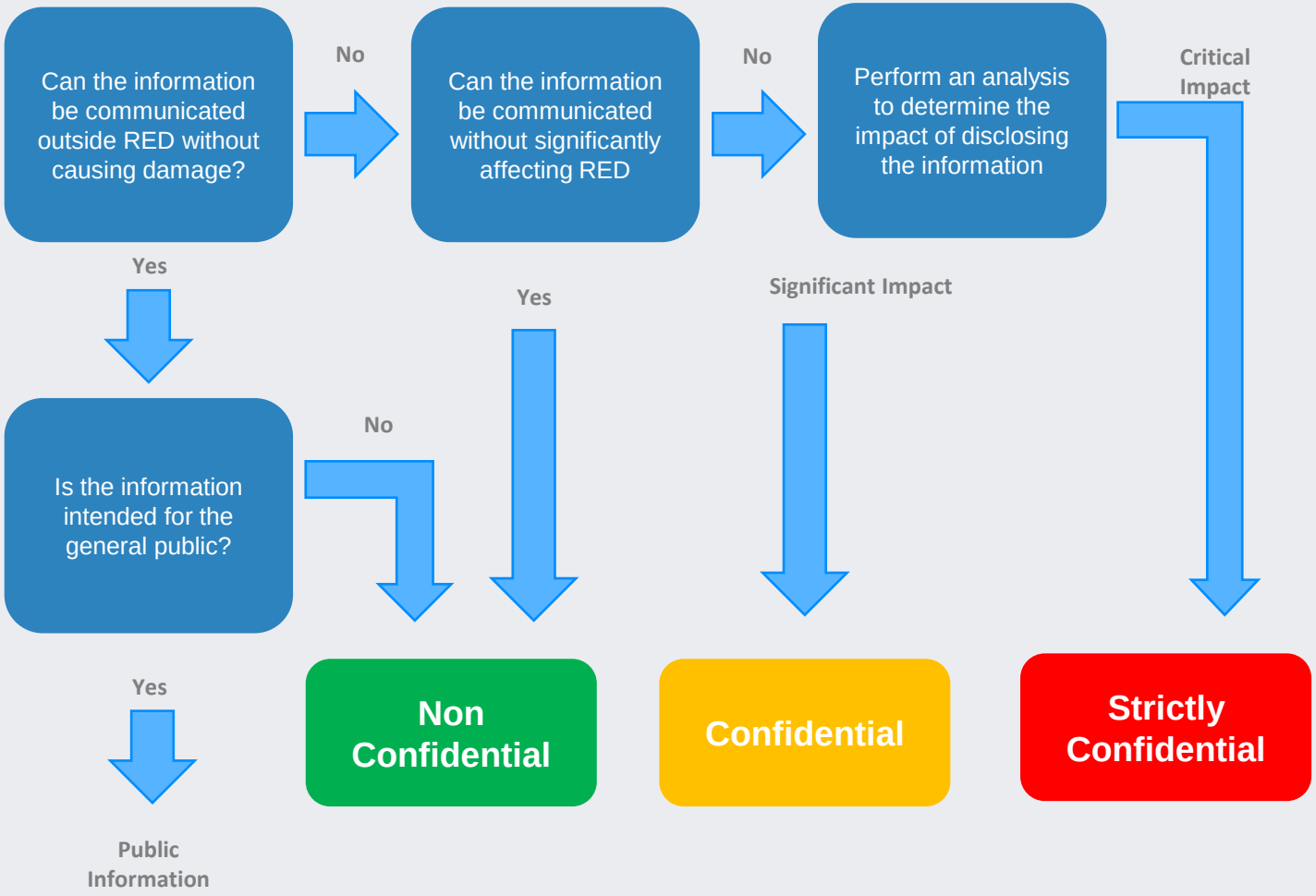
RED

A company of TRACTEBEL ENGIE

RED SECURITY POLICY: CLASSIFICATION OF INFORMATION

Application	Label Name	Data Level (Office Document / Email)			Container Lever (Teams/SharePoint)			Comments
		Encryption	Protection	Permissions	Privacy	External User Access (Teams)	External Sharing	
Word, Excel, PowerPoint	Non-Confidential	✗	✗	N/A	N/A	N/A	N/A	
	Confidential / Confidential (ENGIE Only)	✓	✓	User defined permissions (whoever is selected by the author)	Private by default. Owner can change to public.	✓	✗	Author defines who can read/edit. View content, View rights, edit content, save, print, copy and extract content, allow macros. Limited to authenticated users within ENGIE.
	Confidential / Confidential (ENGIE & Selected Partners)	✓	✓	User defined permissions (whoever is selected by the author)	Private by default. Owner can change to public.	✓	✓	Author defines who can read/edit. View content, View rights, edit content, save, print, copy and extract content, allow macros. Limited to authenticated users within ENGIE and existing guests only.
	Strictly Confidential	✓	✓	User defined permissions (whoever is selected by the author)	Private only	✗	✗	Author defines who can read/edit. View content, View rights, edit content, save, print, copy and extract content, allow macros. Limited to authenticated users within ENGIE.

RED SECURITY POLICY: CLASSIFICATION OF INFORMATION



When choosing between **'Significant/Confidential'** and **'Critical/Strictly Confidential'** levels, the impact matrix must be used to assess what the impact would be if the information were leaked.

Impact	Significant/Confidential Level	Critical (Strictly Confidential Level)
Disruption of the Organisation / staff relations	Disclosure of the information could bring about a risk of labour-related disruptions that could affect RED's productivity and/or the quality of social dialogue, without impacting on other Group entities.	Disclosure of the information could bring about a risk of a breakdown in social dialogue, industrial action or blocking of RED at Group level.
Impact on RED's image	Disclosure of the information could damage RED's image in the eyes of its customers and the public. This also applies to limited leakage of personal data.	Disclosure of the information damage the RED's image and entail major commercial, legal and/or political consequences for the Group. This also applies to large scale leakage of highly sensitive personal data.
Projects lost or jeopardised, financial consequence	Disclosure of the information could affect RED's operational or competitive activities but would not threaten its continued existence.	Disclosure of the information could have such severe effects on RED's– or indeed, the Group's – operational or competitive activities that there would be a serious impact on the results for the financial year

RED SECURITY POLICY: CLASSIFICATION OF INFORMATION

Rules for Managing Classification

The rules below must be applied when handling classified information across its entire life cycle
The IT department defines and provides users with the tools, procedures and training required to implement the rules within the information systems used by employees and during their exchanges with suppliers or partners. It should be noted that compliance with the classification levels also applies to documents outside of RED (following the classification rules of the document owner

Minimum protective measures based on the classification level on the confidentiality scale	Non-Confidential	Confidential	Strictly Confidential
Creation	**Mark ‘’Non-Confidential’’**	**Mark ‘’Confidential’’**	**Mark ‘’Strictly Confidential’’**
Storage Filing	• Store on company-approved IT storage such as OneDrive for Business, SharePoint Online, Teams, or company-managed devices (such as Skynote laptops and company mobile devices) that are protected by ENGIE’s IT teams (multi-factor authentication, contractual security clauses, hard disk encryption etc.). • Storage on personal devices or non-ENGIE approved cloud storage (e.g. DropBox, Google Drive…), is not authorized. Exceptions (e.g. client requirement, partner imposing their cloud solution…) must be subject to prior authorization from management specifying the additional security measures required.	• Keep paper documents in a locked room or secure cabinet. • Use only Applications or IT systems whose security level has been approved by the Cybersecurity teams to handle Confidential data. • Information/data at rest must be encrypted, with the encryption keys either managed by the Cloud Service Provider or by ENGIE. • Authorized technical administrators may access the data for operational or security reasons	• Keep the paper version in a locked cupboard/safe. • Use only Applications or IT systems whose security level has been approved by the Cybersecurity teams to handle Strictly Confidential data and that undergoes regular penetration testing and/or security audits. • Information/data at rest must be encrypted, with the encryption keys managed by ENGIE, not by the Cloud Service Provider. • • Technical administrators may not access the data without formalized authorization
Access Conditions	• Ensure a Non-Disclosure Agreement (NDA) or equivalent contractual confidentiality clause is signed if the information is shared with an external partner. • Multi-Factor Authentication is required to access applications or cloud storage containing ENGIE data.	• User access must be limited to the members of a selected group; access rights must be reviewed on a regular basis. This should be materialized in a dedicated and suitable IT architecture and organization.	• User access is only granted to the authorized recipients who were identified by name. This should be materialized in a dedicated and suitable IT architecture and organization.
Sharing Conditions	• Emails and shared documents (Word, Excel, PowerPoint) must be classified as “Non-confidential” using the ‘Sensitivity’ button in Microsoft Office • The ENGIE-approved solution to share files is OneDrive For Business (the use of non-approved file transfer solutions such as YouSendIt or DropBox is not permitted). For collaborative work on documents, Teams or SharePoint Online • Do not use ENGIE information to feed Artificial Intelligence tools (e.g. GenAI) unless these are explicitly approved and	• Emails and shared documents (Word, Excel, PowerPoint) must be classified as “Confidential” using the ‘Sensitivity’ button in Microsoft Office. That way they are automatically encrypted. • Before sharing the information, identify and verify the group(s) authorized to receive and use it. • Do not share the information outside the authorized group(s) without the approval of a line manager.	• Emails and shared documents (Word, Excel, PowerPoint) must be classified as “Strictly Confidential” using the ‘Sensitivity’ button in Microsoft Office. That way they are automatically encrypted and only the named users can open them. • Identify the authorized recipients by name. Only share with the authorized recipients who were identified by name unless the information owner has given express permission

RED SECURITY POLICY: INCIDENT MANAGEMENT

RISK LEVEL *as defined in the Crisis Management Risk Levels Matrix*	People Health, Safety & Security	Workplace & Office Facilities	Information Security *(including data and company devices/equipment)*
EXTREME	RED Emergency Contact	RED Emergency Contact	RED Emergency Contact
SEVERE	RED Emergency Contact	RED Emergency Contact	RED Emergency Contact
MODERATE	Incident Management Form	Incident Management Form	Incident Management Form
MINOR	Incident Management Form	Incident Management Form	Incident Management Form

PREPARED BY

Shereen Torry

Head of Management Systems & Compliance

For more information about RED, please contact:

Dubai	dubai@red-eng.com	+971 4 297 8846
Istanbul	istanbul@red-eng.com	+90 212 211 9914
London	london@red-eng.com	+44 20 7299 8260
Manila	manila@red-eng.com	+63 2 7950 90 16/7
Newcastle	newcastle@red-eng.com	+44 191 500 3140
Oxford	oxford@red-eng.com	+44 1869 355 600
Singapore	singapore@red-eng.com	+65 6226 3106
Dublin	dublin@red-eng.com	+353 1 661 4420
Cork	dublin@red-eng.com	+353 21 242 8685
Clark	clark@red-eng.com	+63 2 7950 90 16/7
Guildford	guildford@red-eng.com	+44 20 7299 8260

red-engineering

RED_Eng_Design

red_engineering_design

RedEngineeringDesign

RED

A company of TRACTEBEL ENGIE

2024

RED SECURITY POLICY: CLASSIFICATION OF INFORMATION

Emails & Microsoft Office documents – restrictions & protections automatically applied based on the selected classification level (using the “Sensitivity” button in Outlook, Word, Excel and PowerPoint):

Application	Label Name	Data Level (Office Document / Email)			Container Lever (Teams/SharePoint)			Comments
		Encryption	Protection	Permissions	Privacy	External User Access (Teams)	External Sharing	
Outlook	Non-Confidential	☒	☒	N/A				
	Confidential	☑	☑	User defined (email recipients)				Recipients have all usage rights except save as, export and full control. This means they have no restriction (they can forward the email, print or copy from it) but cannot remove the protection. Unprotected office documents attached inherit this protection.
	Strictly Confidential	☑	☑	User defined (email recipients)				Recipients cannot forward the email, print or copy from it. Unprotected office documents inherit the same protection.
	Non-Confidential	☒	☒	N/A	N/A	N/A	N/A	