IT Code of Conduct

Version: 3.3

Restricted

This document is the intellectual property of Kudelski Group and contains proprietary information.

The reproduction, modification, or communication to third parties (or to other than the addressee) of any part of this document is strictly prohibited without the prior written consent.

Table of Contents

GENERAL	
Owner	Group CIO
Reviewers	Group CISO, CIO-Office staff, BU Information Security Officers, Legal, HR representative, and Privacy Manager
Approver	Group CIO
Review frequency	Annually or upon a major change

RELATED DOCUMENTS	
Name	**Location**
Information Security Policy	KG Policies intranet page
Information Classification Policy	KG Policies intranet page
Employee Handbook	HR Global Policies intranet
Endpoint Device Standard	KG IT Policies intranet page
Facilities and Physical Security Standard	KG Policies intranet page
Data Privacy Policy	KG Policies intranet page
Considerations on use of Artificial Intelligence and Chatbots	KG Policies intranet page

DOCUMENT HISTORY				
Version	**Date**	**Changed by**	**Function**	**Description**
1.0	05.MAY.2012	O. Spielmann	Corporate Security	First version.
2.0	21.AUG.2014	L. Vogt	Head of Corporate Security	Second version.
2.1	24.SEP.2014	L. Vogt	Head of Corporate Security	Inclusion of reference to "Règlement Interieur" document from Nagra France.
3.0	04.DEC.2020	T. Corsi	IS Risk & Compliance Manager	Update based on current technology and practices.
3.1	22.OCT.2021	T. Corsi	IS Risk & Compliance Manager	Document review, minor wording changes.
3.1	31 OCT 2022	C. Nash S. Worthington	Group CISO IS Risk & Compliance Analyst	No changes during the year
3.2	2.OCT.2023	O. Spielmann	Group CISO	Addition of document owner, addition of Physical Access, Work from Everywhere and AI & Cloud services acceptable use sections, minor changes.
3.3	21.10.2024	R.Aviolat C.Wolf Mark Beariault	Group CISO ISMS Manager General Counsel, Head of Legal Affairs	Yearly review, precisions on security awareness, added AI risks, minor corrections.

1. Introduction

1.1 Purpose

This Information Technology Code of Conduct (hereinafter, this "IT Code of Conduct") defines the minimum-security standards and behaviors users must comply with when using Group IT Assets.

Should you have questions or comments regarding your activity compliance with this Code of Conduct, contact Corporate Security at corpsec@nagra.com.

1.2 Scope

This Code of Conduct applies to all Kudelski Group employees and all external parties who are granted access to the Group IT Assets.

1.3 Enforcement

This Code of Conduct is part of the "Employee Handbook," which is an integral part of each employee's work agreement.

Violation of this Code of Conduct may lead to disciplinary measures, up to and including termination of employment. In the case of a criminal offense, further measures may be taken.

1.4 Exceptions Management

In countries with local laws regulating Information Security, such local laws take precedence.

Any requested exceptions to this policy must be communicated to and approved by Corporate Security in writing.

1.5 Terms and Definitions

Personal data - any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Endpoint Device – End-user IT devices such as workstations, laptops, tablets, mobile devices, etc.

Group IT Assets – Kudelski Group IT systems and infrastructure, provided by corporate IT or Business Units:

- Endpoint devices such as laptops, workstations, and mobile devices.
- Network environments providing connectivity to internally and externally hosted systems (internet browsing and cloud solutions)
- Unified communications hardware, such as audio and video conferencing solutions.
- Group IT Virtual Assets as defined below

Group IT Virtual Assets - Kudelski Group IT virtual assets and infrastructure provided by corporate IT or Business Units:

- Virtual Endpoint devices, virtual workstations, servers, containers
- Virtual network devices or cloud network devices providing network connectivity and control to internal or external systems
- Virtual unified communications software, such as online collaboration tools and virtual telephony solutions
- Cloud environments such as applications, platforms or infrastructure as a service asset

Group IT Services – Any application, data processing or storage that can be used as a service to deliver the business where the infrastructure and the management of the service is performed or formally cleared by Corporate IT (e.g. Kudelski Group Business unit specific infrastructure with legal and IT reviewed contract and architecture). It includes all types of services such as HR systems, Financial Reporting System, Corporate E-mail, Corporate Cloud, Business Unit specific Production Cloud infrastructure with legal reviewed contract and IT reviewed architecture.

Partner IT Services - Any application, data processing or storage that can be used as a service to deliver the business where the infrastructure and the management of the service is performed by a Kudelski Group Partner, such as a client or a solution supplier. It includes all types of services such as Project Management repository at client, data transfer solutions from clients.

3rd Party IT Services – Any application, data processing or storage that can be used as a service to deliver the business where the infrastructure and the management of the service is performed by a 3rd party and that is not a Group IT Service or a Partner IT Service. It includes all types of services such as SaaS (e.g. online e-mail services, file transfer services, translation services), PaaS (e.g. database as a service) and IaaS (e.g. cloud infrastructure services). Third Party IT services also include Artificial Intelligence Services such as Large Language Model services.

IT Services – IT Services includes all Group IT Services, all Partner IT Services and all 3rd Party IT Services.

2. Policy

2.1 General

It is the responsibility of all users to demonstrate and encourage the behaviors required by this IT Code of Conduct and the other policies and standards published by the Kudelski Group.

2.2 Information protection

Kudelski Group employees are accountable for any information and data stored on their devices.

You are responsible for defining the classification level of the documents you own and labeling and handling them according to the Group's Information Classification Policy.

Only Kudelski Group provided services may be used to store, transfer, or otherwise process Kudelski data. Portable devices should contain a minimum of information and only what is required for current business activities.

When providing access to data to an external party, ensure that such person has been appropriately cleared according to the data's classification level. External contractors are subject to a clearance process and must sign a Non-Disclosure Agreement (NDA) before being granted access. NDAs are provided and managed by the Kudelski Group legal department. The clearance of business partners' employees may be covered by a global contract and is subject to the legal department's review.

When processing company confidential information outside of the Group's premises, you must take reasonable precautions to protect its confidentiality, independently of its form (i.e., electronic, hard copy, or oral).

Processing classified information in IT Services need to follow the handling rules of the information classification policy to avoid unintentionally exposing confidential data to the Internet.

Unless the information is in active use, your desk must be cleared of company confidential or valuable data during non-working hours and all information locked away. You must lock or log out of your session before leaving your computer or mobile device unattended. Punctual clear desk policy audits will be run in the premises of Kudelski Group.

2.3 Security Awareness

Kudelski Group employees are our first line of defense against cyber-attacks. Setting you up for success includes providing you sufficient information, training and exercises on the latest attack techniques and updated policies.

It is the responsibility of every employee to:

- Understand the official corporate communications to be aware of the latest changes, planned downtimes and security risks
- Follow the mandatory security awareness training and pass the associated tests within three months. There are two different security trainings that employees are expected to complete:
    - Security Fundamentals: All new hires are required to complete this training during onboarding, except in extreme or specific cases of “force majeure.”
    - Security refresher or additional required training: Given the dynamic nature of staffing (arrivals/departures), achieving an 80% completion rate across the entire workforce is considered a success. To continuously assess our resilience to cyber-attacks, the Group will organize attack simulation exercises, which may involve you randomly. Not performing the mandatory security training may prevent you accessing critical Group services and infrastructure or even lead to your account disablement.

2.4 Physical Access

Physical security remains central in information security concepts. Several protections may become inefficient in case the threat actor is getting physical access to the systems or information.

Kudelski Group employees are provided an access solution (e.g. badge, key, other access media) for physical access to the Group offices.

Sharing or lending access solutions is strictly forbidden. In case an access solution such as a badge, key or other media is lost, stolen or is suspected to be lost or stolen, an immediate report to the local facilities management unit is required.

In case a Kudelski Group employee is receiving guest(s) in the office, it is the responsibility of the employee to:

- Follow the local office visitor policy, perform the registration and obtain valid access badge(s)
- Accompany visitor(s) within the office during the stay until visitor(s) quit the facilities

2.5 Work from Everywhere

With the remote work capabilities and mobility needs, working from outside the Company premises is widely adopted for travel, client support or teleworking needs. The Work from Everywhere model includes Work from Home, Work from public locations and Work from another company premise.

When authorized by your local policy, the Work from Everywhere model must ensure the continued protection and confidentiality of the Group information. It is the responsibility of the employee:

- Protect information from theft, access or duplication. Especially unattended devices should be protected appropriately (e.g. hotel safe).
- Use only encrypted media for storage of Confidential information
- Not execute Secret level work outside of cleared areas (i.e. Kudelski Group secured areas, client secured areas)
- Not store information outside validated platforms and solutions provided by the Group
- When connected to untrusted networks in public areas (e.g. hotels, airports), privilege always-on VPN secure connection to execute business work
- Report immediately any suspected or confirmed security incident to your local IT help-desk

2.6 Information System Access

Cyber-attacks often identity theft and impersonation techniques (e.g. phishing). Being cautious when being prompted to provide a username or password or to validate an access from a smartphone, reduces drastically the risk of being impersonated.

You must comply with the Group's password and authentication requirements to properly handle your systems access.

Your login ID, passwords, and authentication tokens are strictly personal and must not be written down or shared with anyone, including Corporate IT, other support staff, or external parties. If you need to share access with a fellow worker, contact Corporate IT to give your colleague the necessary access with the data owner's approval or use application-specific mechanisms for access delegation.

You are expected to enable multi-factor authentication (MFA) at the start of your employment and maintain it for the duration of your work at the Kudelski Group. This applies to your Kudelski Group personal account and any accounts where multi-factor authentication is supported. If you receive an unexpected authentication validation on your smartphone, don’t approve it. It could be a threat actor attempting to impersonate you.

If you are a system administrator with privileged access to Group IT Assets, ensure that the privileged access is only used to carry out administrative activities such as installing software or making configuration changes.

2.7 Acceptable use of Group IT Assets

Kudelski Group provides you with Group IT Assets for your work and in a manner that supports the Kudelski Group's mission. It is not allowed to purchase IT Assets to perform your job and expense them to the company. If you require new hardware to perform your work, a request should be made to Corporate IT or approved by respective Business Unit management.

You are entitled to use the Group IT Assets to perform your work and use the software available in the Corporate IT Software Service catalog. Corporate IT maintains a list of available software in the Service Portal (Service Now), which can be installed upon request; if you require new software to be authorized for business purposes, a request should also be made to Corporate IT.

Occasional personal use of the Group IT Assets assigned to you, and the Internet is allowed, provided it does not disrupt any business activity or incur additional costs to the Group.

The following use of the Group IT Assets are not permitted and subject to disciplinary measures:

a) access, upload, download, store or distribute offensive, derogatory, defamatory, sexual in content, or otherwise inappropriate in a business environment.

b) transmit obscene, libelous, abusive, sexually explicit, threatening, or harassing statements to another employee, client, vendor, or other outside parties.

c) violate any applicable local or international law.

d) vandalize, damage, or disable the property of another individual or organization.

e) impersonate other users' accounts, compromise, or circumvent standard security configuration and settings, including but not limited to authentication mechanisms, hacking tools, and vulnerability exploits.

f) Change your computer's standard security configuration and settings unless you have been officially mandated and authorized to do so by Corporate Security

g) violate copyright, licenses or otherwise use the intellectual property of another individual or organization without permission.

h) generate personal costs through Corporate provided assets and service subscriptions. (ex. Media downloads, application subscriptions, gaming purchases, etc.)

i) conduct revenue-generating activities unrelated to Kudelski Group.

j) Employees are not permitted to utilize penetration testing or vulnerability scanning tools on the Group's networks without validating with the Corporate Security department. This includes hiring outside firms to perform these types of tests.

k) Use 3rd Party IT Services for classified information not following the information classification policy

2.8 Acceptable use of personal endpoint devices

In addition to the requirements in this IT Code of Conduct**,** the use of personal endpoint devices is allowed if it meets the following criteria:

- It is used only to send and receive a limited set of corporate data such as electronic mail, calendar, contacts, and tasks.
- You accept the installation of an Endpoint Device Management agent that will enforce security policies.
- You ensure that your device prevents unauthorized access via a password or PIN code when unattended
- You ensure that stored data is encrypted.
- You accept that access to corporate data from a Personal Endpoint Device is monitored.
- In cases of confirmed information security incidents associated with the personal device, you agree to allow the security department access to the device if necessary for investigations and prevent it from accessing corporate data and delete corporate data stored if applicable.
- You accept that Corporate IT may ask for the removal of a personal application software if that opposes a threat to corporate data stored in the device; Corporate IT may delete corporate data stored on the Personal Endpoint Device.
- You must report to IT Helpdesk if the Personal Endpoint Device with corporate data is lost or stolen. In such

events, Corporate IT will attempt to remotely wipe (reset or data deletion), resulting in partial or complete personal data loss.

2.9 Protection of assets

You are responsible for using the Group IT Assets in a way that does not compromise their proper functioning or expose them to risks. In case of doubt, consult with Corporate IT.

If you are issued a Kudelski portable (laptop, tablet) computer, you must take reasonable precautions. When out of the office, the device should always be under your direct control and not used by non-Kudelski Group users, including friends or family members. When left out of sight, it must be stored in a secure location.

You should not connect your device to a public USB charging station without using a USB data blocker. If you have questions on this, please reach out to Corporate Security.

Any lost or stolen device with Kudelski Group data must be reported immediately to the IT Helpdesk.

In the event of employment termination, you must return to Corporate IT any Group IT Asset assigned to you without erasing the stored data, including corporate mobile devices and SIM cards, for secure data disposal and hardware re-use/decommission. You must also work with the Corporate IT team to remove your iCloud account from any Apple devices you were issued.

2.10 Use of Internet and communications systems

Exercise good judgment when using Kudelski provided communications systems and be conscious that information that you download, create, store, send, or share has a cost. Inappropriate use of communication systems may have negative consequences, including legal or compliance issues and damage to Kudelski's reputation.

When communicating publicly on the Internet (i.e., using mailing-lists, forums, social networking sites, etc.) in the context of conducting your professional activity, clearly indicate that the opinions expressed are your own and not those of the Group (unless you have been expressly designated as a spokesperson of the Group). Only information classified as PUBLIC may be disclosed when using such communication services. If you desire to post things on behalf of the Group, please contact your respective entity's marketing department.

- When communicating outside of the company, don’t disclose employees’ email addresses when forwarding emails or replying to public mailing lists.

Corporate E-mail and web conferencing systems must be used for business purposes only. The use of a private E-mail address for your personal communications is allowed.

Be mindful when using any tool or functionality to record live presentations, streaming video, telephone calls, and other presentation content. You must only use voice, video, or screen recording features if:

- it is not performed from high security areas where the practice is prohibited.
- it is used for internal collaboration, training, or marketing/sales purposes.
- you remain responsible for recording secure storage and retention for as long as it is relevant.
- if all recorded session participants acknowledge and agree that the session will be recorded, explaining the purpose of the recording and the location it will be stored.

2.11 Acceptable use of Artificial Intelligence and Cloud services

Cloud services are needed to support Kudelski Group business, including artificial intelligence (AI) and Large Language Models (LLM). However, acceptable use rules and guidelines are required to keep our information protected while benefitting from these technologies. (Ref: Responsible AI guidelines)

Acceptable Use could be, but is not limited to, the following business supporting purposes: improving written texts, translations, writing documentation or papers outline guidance, academic research and personal productivity.

When using AI or LLM’s, consideration must be given to the following risks:

- Factual Inaccuracies
- Hallucinations – completely invented output
- Outdated Information
- Biased Information
- Copyright Violations
- Concern about AI becoming less reliable as people feed it false information
- Providing sensitive information to non-IT approved providers

IT Services can be used unrestrictedly with public non identifying data. For non-public data, please refer to the Information Classification Policy guidelines. For Personal data, IT Services usage should adhere to the Data Privacy Policy and Privacy Committee's Considerations on use of Artificial Intelligence and Chatbots. All use of AI should be done in accordance with the Group Responsible AI guidelines.

3rd Party IT Services usage for AI are strictly prohibited if any of the following information are involved:

- Any type of Personally Identifiable Information
- Any information contained in an NDA
- For any information or data classified, handling requirements are defined in the Information Classification Policy
- Any Copyrighted or Trademarked information pictures or data
- Any information regarding products not released

In addition, as a general guideline, make sure that you submit sanitized data to 3rd Party IT services by, but not limited to:

- Removing all references to Kudelski Group and its affiliates when content is submitted.
- Removing all references to products in development and not released.
- Avoiding providing specific content that could reveal patentable ideas and/or domains of research.

As the domain is dynamic and evolving, make sure you always refer to the latest version or the Group Responsible AI Guidelines.

2.12 Reporting Security Events and Incidents

You are responsible for reporting as soon as possible to Corporate Security any abnormal or suspicious events on any Group IT Assets you have access to. Please use corpsec@nagra.com or (https://kudelskigroup.service-now.com/kudelski).

3. Monitoring and Privacy

All IT components (servers, networks, applications, e-mail, Internet, etc.) produce network traffic and audit trails (log files) which are kept securely for a maximum of two years or until the system has reached its storage capacity, whichever occurs first. Kudelski Group IT Assets are subject to automated and manual monitoring to detect security threats preventing IT services disruptions, and for capacity planning and resource allocation purposes.

Employees shall cooperate with Corporate Security on events or investigations associated with information security incidents.

Some identification data (login name, device name, network address) may be processed in case of necessity to allow authorized Kudelski Group staff or authorized third parties to perform targeted investigations. It also may become necessary for the security team to access your corporate devices and communication accounts. This would be the case in the event of a service disruption, a suspected security breach, suspicion of fraudulent or illegal activities, abuse of the Kudelski Group IT Assets, or any misconduct.

Corporate IT will not disclose personal data to third parties without the consent of the data owner following strict Corporate guidelines and subject to the approval of the Group's General Counsel or unless required by law or authority.