Consultant Commitment Charter

Objective

This Consultant Commitment Charter defines the security, compliance, and responsible usage rules that every consultant must acknowledge and adhere to when assigned to a Marionnaud project.

Consultants are individually responsible for protecting Marionnaud's systems, data, and reputation.

Non-compliance may result in immediate removal from assignment and further contractual or legal actions.

1. Equipment usage

- Consultants must exclusively use Marionnaud-provided IT equipment (laptops, phones, tablets, ...).
- Personal or BYOD (Bring Your Own Device) equipment is strictly prohibited.
- Marionnaud corporate tools (e.g., Microsoft 365, Wrike) must not be accessed from non-Marionnaud or personal devices.
- Consultants are not granted administrator rights on their laptops or devices.
- Consultants must not attempt to bypass, escalate, or modify device security settings to gain administrator access.
- Any required installation or technical configuration must be requested through the Marionnaud Digital Workplace team.
- All devices must be kept updated, and consultants must promptly apply software patches and reboot as necessary.

2. Data Protection

For the purpose of this Charter, the term **Information Systems** covers **all types of information assets and infrastructures** owned, controlled, or processed by Marionnaud, including:

- **Electronic forms** (e.g., computers, servers, emails, databases, cloud platforms),
- **Physical forms** (e.g., printed documents, handwritten notes, storage media),
- **Verbal communication** (e.g., discussions, telephone conversations, meetings),
- **Any other medium** by which information is created, shared, stored, or transmitted.

- Consultants must not copy, transfer, extract, or leak any data outside Marionnaud's Information Systems.
- No use of USB drives, external storage devices, or unauthorized data transfers is permitted.
- Navigation to suspicious websites is forbidden (examples: gambling, pornography, weapons, hacking, and other unrelated content).
- Consultants must handle incoming external data with extreme caution (e.g., email attachments, external drives).

In this context, the protection of personal data is particularly important.
Therefore, consultants must strictly adhere to the requirements set forth by the General Data Protection Regulation (GDPR).

- Consultants must protect all personal data they may access in the course of their missions.
- Personal data must be processed strictly for the intended professional purpose, under Marionnaud's instructions.
- Unauthorized access, use, disclosure, or storage of personal data is strictly prohibited.
- Consultants must comply with the GDPR (General Data Protection Regulation) principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.
- Any potential data breach must be immediately escalated following Marionnaud's incident management process.

3. Security Awareness

- Consultants must complete Marionnaud's mandatory cybersecurity e-learning **quarterly**.
- Consultants must remain vigilant against phishing and other social engineering attacks.
- Participation in simulated phishing exercises is mandatory.

4. Incident Management

- Any suspicious behavior, technical anomaly, potential data leak, or security incident must be **immediately reported** by either:
    - Sending an email to **cybersecurity@marionnaud.com**
    - Opening an ITSM ticket through the Marionnaud internal system.

5. Professional Conduct

- Consultants must behave responsibly and ethically, in line with Marionnaud's Code of Conduct (cf Appendix 5)
- Excessive internet use for personal purposes during working hours is prohibited.
- Consultants must protect physical assets (laptops, phones, tablets) from theft, damage, and misuse at **all times**.

6. Annual Review

- This Consultant Commitment Charter is reviewed **once per year** by Marionnaud.
- If updates are made, the provider must ensure that each assigned consultant re-signs the latest version.

7. Acknowledgment and Termination Clause

By signing this document, the consultant confirms their **full understanding** and **acceptance** of the above obligations.

Date :

Signature :