**PPIT Questionnaire**

**Questionnaire on Cyber Security Practices in NADRA**

***Company's Approach to Cyber Security:***

1. How integral is Cyber Security within NADRA operations and objectives?

­­­­­­­­­

1. Are there dedicated teams or departments solely focused on Cyber Security within the company?
2. How does the company stay updated with evolving Cyber Security threats and trends?
3. Are there specific policies or frameworks in place to address Cyber Security concerns within the company?
4. How often are employees trained or updated on Cyber Security best practices and protocols?

***Cyber Security Measures and Protocols:***

1. Can you outline the primary Cyber Security measures implemented within NADRA?
2. What encryption standards or protective measures are employed for sensitive data handling?
3. How does the company manage access control and authentication for its systems and networks?
4. Are there regular audits or assessments conducted to evaluate the effectiveness of Cyber Security measures?

***Incident Response and Recovery:***

1. How does NADRA handle Cyber Security incidents or breaches?
2. Can you share any instances where the company effectively responded to a Cyber Security incident?
3. What protocols or procedures are in place for data recovery and system restoration post a security breach?

**Employee Training and Awareness:**

1. How are employees trained or educated about Cyber Security best practices within the company?
2. Are there initiatives in place to raise employee awareness regarding social engineering attacks or phishing attempts?
3. Does the company conduct mock drills or simulations to test employee responses to Cyber Security threats?

***Third-Party Vendors and Partnerships:***

1. How does NADRA ensure Cyber Security compliance among third-party vendors or partners?
2. Are there specific criteria or assessments conducted before engaging with third-party vendors concerning their Cyber Security measures?
3. What measures are in place to protect the company's data when shared with external collaborators?

***Data Privacy and Compliance:***

1. How does the company ensure compliance with data privacy regulations (such as GDPR, CCPA, etc.)?
2. Are there specific protocols to handle customers' personally identifiable information (PII)?
3. What steps are taken to regularly review and update data privacy policies in accordance with changing regulations?

***Security Infrastructure and Technology:***

1. Can you outline the current Cyber Security infrastructure and technologies utilized by NADRA?
2. How often are security systems and technologies updated or upgraded to address new threats?
3. What measures are in place to secure the company's network and infrastructure against cyber threats?

***Risk Management and Assessment:***

1. Does the company conduct regular risk assessments or vulnerability scans to identify potential threats?
2. How are risks prioritized and mitigated within the Cyber Security framework?
3. Are there contingency plans in place to address potential Cyber Security risks or emergencies?

***Compliance with Industry Standards:***

1. Does NADRA adhere to specific Cyber Security standards (e.g., ISO 27001, NIST, etc.)?
2. How does the company ensure alignment with industry best practices and standards in Cyber Security?
3. Are there certifications or audits conducted to validate the company's adherence to Cyber Security standards?

***Collaboration and Reporting:***

1. How do different departments within NADRA collaborate on Cyber Security issues?
2. Is there a designated reporting structure for Cyber Security concerns or incidents within the company?
3. How transparent is the communication regarding Cyber Security incidents to stakeholders and clients?

***Incident Response Evaluation:***

1. Can you discuss the post-incident analysis process after a Cyber Security event?
2. Are there specific learnings or improvements identified from previous Cyber Security incidents?
3. How does the company ensure that the same vulnerabilities or weaknesses aren't exploited again?