Company's Approach to Cyber Security:

How integral is Cyber Security within NADRA's operations and objectives?

Essential; integral to safeguarding national identity data.

Are there dedicated teams or departments solely focused on Cyber Security within the company?

Yes, specialized Cyber Security teams in place.

How does the company stay updated with evolving Cyber Security threats and trends?

Regular monitoring, industry collaboration, and threat intelligence.

Are there specific policies or frameworks in place to address Cyber Security concerns within the company?

Yes, comprehensive Cyber Security policies and frameworks established.

How often are employees trained or updated on Cyber Security best practices and protocols?

Regular training sessions to keep employees updated.

Cyber Security Measures and Protocols:

Can you outline the primary Cyber Security measures implemented within NADRA?

Encrypted databases, stringent access controls, multi-layered security.

What encryption standards or protective measures are employed for sensitive data handling?

AES encryption for sensitive data protection.

How does the company manage access control and authentication for its systems and networks?

Multi-factor authentication, role-based access controls.

Are there regular audits or assessments conducted to evaluate the effectiveness of Cyber Security measures?

Yes, periodic audits to assess Cyber Security effectiveness.

Incident Response and Recovery:

How does NADRA handle Cyber Security incidents or breaches?

Immediate incident response protocols activated.

Can you share any instances where the company effectively responded to a Cyber Security incident?

Confidential; responded promptly to mitigate risks.

What protocols or procedures are in place for data recovery and system restoration post a security breach?

Backup systems and disaster recovery plans in place.

Employee Training and Awareness:

How are employees trained or educated about Cyber Security best practices within the company?

Regular training sessions and awareness programs.

Are there initiatives in place to raise employee awareness regarding social engineering attacks or phishing attempts?

Yes, ongoing awareness campaigns against phishing and social engineering.

Does the company conduct mock drills or simulations to test employee responses to Cyber Security threats?

Regular simulated drills to test employee readiness.

Third-Party Vendors and Partnerships:

How does NADRA ensure Cyber Security compliance among third-party vendors or partners?

Stringent Cyber Security requirements for third-party vendors.

Are there specific criteria or assessments conducted before engaging with third-party vendors concerning their Cyber Security measures?

Yes, thorough assessments of third-party Cyber Security protocols.

What measures are in place to protect the company's data when shared with external collaborators?

Secure data sharing protocols and encryption.

Data Privacy and Compliance:

How does the company ensure compliance with data privacy regulations (such as GDPR, CCPA, etc.)?

Adherence to local and international data privacy laws.

Are there specific protocols to handle customers' personally identifiable information (PII)?

Strict protocols for handling and securing PII.

What steps are taken to regularly review and update data privacy policies in accordance with changing regulations?

Regular policy reviews to ensure compliance with changing regulations.

Security Infrastructure and Technology:

Can you outline the current Cyber Security infrastructure and technologies utilized by NADRA?

Cutting-edge technologies; sophisticated infrastructure.

How often are security systems and technologies updated or upgraded to address new threats?

Continuous updates to adapt to evolving threats.

What measures are in place to secure the company's network and infrastructure against cyber threats?

Firewalls, intrusion detection systems, and continuous monitoring.

Risk Management and Assessment:

Does the company conduct regular risk assessments or vulnerability scans to identify potential threats?

Regular risk assessments and vulnerability scans.

How are risks prioritized and mitigated within the Cyber Security framework?

Risk-based approach to prioritize and mitigate vulnerabilities.

Are there contingency plans in place to address potential Cyber Security risks or emergencies?

Detailed contingency plans for Cyber Security emergencies.

Compliance with Industry Standards:

Does NADRA adhere to specific Cyber Security standards (e.g., ISO 27001, NIST, etc.)?

Adherence to industry-standard Cyber Security protocols.

How does the company ensure alignment with industry best practices and standards in Cyber Security?

Continuous alignment with best practices through audits and reviews.

Are there certifications or audits conducted to validate the company's adherence to Cyber Security standards?

Regular certifications and audits to validate compliance.

Collaboration and Reporting:

How do different departments within NADRA collaborate on Cyber Security issues?

Inter-departmental collaboration and information sharing.

Is there a designated reporting structure for Cyber Security concerns or incidents within the company?

Clear reporting channels for Cyber Security concerns/incidents.

How transparent is the communication regarding Cyber Security incidents to stakeholders and clients?

Transparent communication to stakeholders as per policy.

Incident Response Evaluation:

Can you discuss the post-incident analysis process after a Cyber Security event?

Detailed post-incident analysis to strengthen protocols.

Are there specific learnings or improvements identified from previous Cyber Security incidents?

Continuous improvements based on incident analyses.

How does the company ensure that the same vulnerabilities or weaknesses aren't exploited again?

Remediation of vulnerabilities to prevent future exploits.