**Cybersecurity Audit Report**

**Organisation: Oil and Gas Free Zones Authority**

**Executive Summary**

The cybersecurity audit was conducted in my role as the Senior IT Engineer (Cloud/Cybersecurity) of the Oil and Gas Free Zones Authority (OGFZA) to assess the effectiveness of the Authority existing cybersecurity program and ensure that the measures required to improve the security posture are implemented. The audit was performed in accordance with the industry standards and regulations, including National Information Technology Development Agency’s Guideline for government MDAs and the National Data Protection Bill (NDPB) Regulation.

**Scope**

The audit covered the following areas of the organization’s security program:

* Data security practices
* Software and hardware performance
* Regulatory and legal compliance status
* Vulnerabilities affecting the ecosystem
* Effectiveness of existing security policies and procedures
* The presence of internal and external threats

**Methodology**

The audit was conducted using a combination of manual and automated techniques. The manual techniques included interviews with key personnel, review of policies and procedures, and physical inspections. The automated techniques included vulnerability scanning, penetration testing, and network security assessments.

* **Data security practices**: This area was assessed by reviewing the organization’s data security policies and procedures, as well as conducting interviews with key personnel. The audit also included a review of the software and hardware performance to ensure that the data is being stored and transmitted securely.
* **Software and hardware performance**: The audit used automated techniques such as vulnerability scanning, penetration testing, and network security assessments to assess the software and hardware performance of the organization’s systems.
* **Regulatory and legal compliance status**: The audit assessed the organization’s compliance with industry standards and regulations such as NITDA’s Guideline for government MDAs and NDPB. This was done by reviewing the Authority’s policies and procedures, as well as conducting interviews with key personnel.
* **Vulnerabilities affecting the ecosystem**: The audit used automated techniques such as vulnerability scanning and penetration testing to identify vulnerabilities in the Authority’s systems.
* **Effectiveness of existing security policies and procedures**: This area was assessed by reviewing the Authority’s security policies and procedures, as well as conducting interviews with key personnel.
* **The presence of internal and external threats**: The audit used automated techniques such as network security assessments to identify the presence of internal and external threats.

**Findings**

The audit revealed that the Authority’s cybersecurity program is ineffective in managing cyber risks. Fundamentally, the following issues were prominent:

* Lack of awareness among employees about cybersecurity risks
* Inadequate security controls for remote access
* Inadequate security controls for mobile devices
* Inadequate security controls for third-party vendors

**Recommendations**

Based on the findings of the audit, the following recommendations were made:

* Develop and implement a cybersecurity awareness training program for all employees
* Implement two-factor authentication for remote access
* Implement mobile device management policies and procedures
* Implement vendor risk management policies and procedures

**Conclusion**

The cybersecurity audit provided valuable insights into the Authority’s cybersecurity program and identified areas that required improvement. The recommendations made in this report helped the Oil and Gas Free Zones Authority to improve its security posture and manage cyber risks effectively.