**PREPARATION OF A CYBERSECURITY INCIDENT RESPONSE REPORT**

**ORGANISATION: OIL & GAS FREE ZONES AUTHORITY**

**Incident Summary**: On January 23, 2021, at approximately :00 AM, in my role as the Senior IT Engineer (Cloud/Cybersecurity) for Oil and Gas Free Zones Authority, while conducting routine security audit, I detected a cyber security incident involving the compromise of several email accounts. The attack was initiated through a phishing email that appeared to be from a trusted source. The email contained a malicious attachment that, when opened, installed malware on the user’s computer. The malware then allowed the attacker to gain access to the user’s email account.

**Impact Assessment**: The attack affected a total of 48 email accounts, including those of several senior executives, Financial Controller, being one of them. The attacker was able to access sensitive information, including confidential emails and attachments. The attacker also used the compromised accounts to send phishing emails to other employees within the Authority, and also sent emails to other sister organisations with have working relationships with.

**Incident Containment**: Upon detection of the incident, I immediately disabled the compromised accounts and isolated the affected systems. I also implemented additional security measures, including the deployment of anti-malware software for the endpoint devices in the Authority. I enforced the implementation of two-factor authentication for all email accounts.

**Incident Investigation**: I conducted a thorough investigation of the incident, including the analysis of the malware and the identification of the attacker’s IP address. The investigation revealed that the attacker was a member of an organized cybercrime group based in Pakistan.

**Incident Remediation**: I implemented remediation measures by restoring affected systems and recovering lost data. I also implemented additional security measures to prevent future incidents, including the deployment of intrusion detection and prevention systems. I installed Advanced Threat Protection (ATP) in our email server.

**Incident Reporting**: I reported the incident to the Head of IT Department and notified all affected parties, including senior executives and employees whose email accounts were compromised. The IT department also communicated the incident to the Authority’s stakeholders and provided guidance on how to prevent similar incidents in the future.