Information Security Policy

- UHP – IT maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that:
  - Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organization using administrative, physical and technical controls.
  - Provide value to the way we conduct business and support institutional objectives.
  - Comply with all regulatory and legal requirements, including: (adjust as appropriate).
    - Information Security best practices, including ISO 27001 and ISO 27002.
    - Contractual agreements.
    - All other applicable legal laws or regulations.
- UHP - IT provides entire IT application and infrastructure support to UHP and UHP - IT security team is responsible to Implement, maintain and monitor the information security management processes within UHP.
- All UHP employees, customers, contractual third parties, service providers, consultants and any other parties are responsible for protecting UHP information and Information processing facilities from all threats, whether internal or external, deliberate or accidental.
- All UHP employees, contractual third parties, service providers, consultants and any other party are responsible to sustain high level information security posture within the organization with preserving the confidentiality, integrity and availability at any given time.
- Each IT application, system and infrastructure device owned by the UHP will have nominated users who will have day-to-day responsibility for complying with information Security Policy on that system.
- Safety of company provided Personal Computers (PC) and IT Peripherals (i.e.: mobiles, Tablets, etc.) will be the responsibility of each individual user.
- UHP - IT management, employees, contractual third parties, service providers, consultants and any other party to maintain an appropriate level of awareness, knowledge and skill to allow them to minimize the occurrence and severity of information security Incidents.
- Third-party service providers who are responsible to provide and maintain IT services, system, or infrastructure devices/services on behalf of the UHP,

responsible for complying with and maintain UHP - IT Information Security policy requirements.

- UHP - IT shall consider and assess the information security aspects during the IT projects that connect with IT environment and services.
- UHP - IT shall responsible to minimize internal and external information security risks to the acceptable level. This will include, ensuring that adequate information security risk management practices within the UHP.
- UHP - IT shall be responsible to minimize information security incidents at an acceptable level and ensure that adequate incidents management (e. Incident are identified, recorded and responded) in a timely manner.
- UHP - IT is committed to continually improve the sustainability, adequacy and effectiveness of information security management system.
- UHP - IT shall maintain the compliance effect to the information security management with any applicable legal, regulatory and contractual obligations while preserving UHP reputation and image.
- Breaches of Information Security Policy shall be considered as a violation and UHP – IT or HR shall take required actions against responsible parties. This may lead to disciplinary action against the employee who violates the Policy and is applicable to third parties/contractors service level agreement as well. The level of disciplinary action will be in accordance to the Human Resources policies and this could be a minor/major/grave offense depending on the gravity of the violation.
- The information security program is reviewed no less than annually or upon significant changes to the information security environment.

Chief Executive Officer

Umm Al Houl Power Company

11th September 2024