Derman Sanchez-Amaya

Chief technology Officer

D.A.S.A Consulting Firm

Firms Purpose: D.A.S.A Consulting Firm is a Small Company in the middle East, Egypt consisting of 25 IT specialist members. As an IT Consulting firm we strive to providing Technological Analysis to any corporation, Business and Private Sectors to avoid and prevent Technological breaches and cyber attacks.

D.A.S.A Scope: The D.A.S.A policies **MUST** be followed by all our Contractors, Volunteers and partners as long as they are using any of our Hardware or System outside or inside the workplace with no Exception(Note: No Volunteers shall be allowed to take any System or Hardware out the work place.

Policies Elements

Data Confidentiality: All data security and Confidentiality is the most Valuable asset within our Company and it must be protected.

- Workers/ Volunteers personal Information
- Partners/Contractors Confidential Data
- Financial Information
- New Projects and old Projects confidentiality

All employees, partners, and Contractor are responsible for their missed use of the firm's technological hardware and system and are In notice of the risk of their own data Usage in prospect to Our Data Confidentiality policy.

Data Protection: All our systems are hardwares are Under Technology protection. However, is Also your duty as an Employee, Volunteer and partner to assure the maximum Level of Security possible for our Firm and Partners:

- All Firm Technology Equipment must be kept within the Maximum secure network range(Unless Clearance is granted by the CFO)
- All Firm Official Account must long off before the Building.
- All Personal Computer/ Tablets must be turned off before leaving the Building and left in the firm Secure Compartments to charge.
- NEVER LOG IN WITH EXTERNAL DEVICE TO THE COMPANY'S NETWORK.

Official Clearance: The Company is developed in a hierarchy System to Prevent unwanted Data assesses and Miss usage and all Employees Under the Hierarchy System must follow its Infrastructure with No exception.

- All Unclearance must ask for clearance when Needed.
- All employees in a highers Hierarchy Must never disclose personal Information with downlines. Failure to do so will enter a legal matter of Policy violation.
- All Clearance requests have to be notified to the CFO when the CFO is not present the Vice presidents must be Notify.

Emails: All Workplace Emails Shall only be used for the Firms Necessities and must be kept secure at all times.

- Must not Access Email in an unprotected device.
- Email password should be Kept strong and not personal.
- **Avoid Clicking on Hyperlink or any non-Business related Emails.**
- Report, all Scams and breaches and Suspicious behavior.

Data Transfer: All Personal or Sensitive Data transferring Must done Under Secure passpath.

- Personal Data Must never be disclosed through Firms Emails.
- All Tranering Firm Data Must be disclosed By the Hierarchy and carefully evaluated by two or more individuals
- Never Disclose any firm Information Through any Outsource network but the secure Firm Network.

Anti Viruses: All D.A.S.A Firm related Devices must be kept under the D.A.S.A Anti-Virus Protection at all Times.

- All Devices Should be Under Anti-Virus Protected Failure to do puts all the Infrastructure Under risk.
- You should have Ensure your device is Under protection

Failure to do so will put In jeperdy all the Firm's Assets.

Ethernet Assess Policy: All Internet Connection is granted to a Higher up in the Hierarchy to assure the Maximum Level of Cyber safety.

- Internet Passwords Must not be Disclosed to Non- Elegibles.
- Wifi Clearance is Needed at all Times.
- Manager must Input Password.

Software Updates: Technological Equipment shall be kept up to date to avoid any Technological breach that will put in jeopardy the Safety of the firm and Our partners

- All Technological Equipment Shall be keep updated.
- All Updates must be done by Clear Members.
- All Updates Must be granted the Updated flag by the CFO.

Disciplinary Action: All Actions not not meet one of the Policies above shall be followed with a Disciplinary action:

- Highy Severe actions, Includes lawsuits and possible jail time against the intentional Disclosure of the Firms Information.
- Severe: Includes the Miss usage of firms material and resources that will put the Firms intern Network at risk(Fire)
- Bad: The usage of Equipment without proper care. For instance not logging off and not taking proper measurements towards the safety of the firm.

Personal Requirements: All members of the firm must have integrity towards what you might not know regarding a subject or skill.

- Private Lesson must be Taken if a subject is weak or not practical to the overall progress of the firm(Free)
- Must be Honest about the Lack of certain Skill is not punishable but is for the best of the company.
- The better you are the more you get paid ! Therefore, there is always time for improvement and Integrity.