IT Policies

Dawood Equities Limited

http://www.dawoodequities.com

FOREWORD

DEL seeks to establish it's self as a leader over local competition by the innovative use of Information Technology, which in turn will provide its clients/customers with an advantage over their competitors.

The DEL IT policy has been drafted in an attempt to create a comprehensive document, which imbibes the aims and goals of the IT Department as well as defines the progressive attitude the company seeks to formulate in the use of modern IT procedures.

The Policy provides concise guidelines to non-technical staff with regard to the correct and most constructive usage of IT elements.

To obtain the maximum benefit from this technology, managers and all the staff are encouraged to understand the benefits of IT strategy and policy, and to apply its content in a consistent format across the organization.

In keeping with this all IT matters shall always be referred to IT and all external communications related to IT matters shall be through IT.

Chief Executive Officer

DEL Computer Guidelines and Policies

TABLE OF CONTENTS

1. OBJECTIVES: 5

2. ORGANIZATION STRUCTURE: 6

3. IT INFRASTRUCTURE:. 6

4. COMPUTER STANDARDS: 7

4.1 Computers: **. 7**

4.2 IBM Computer Specifications: **. 8**

4.3 Network Specifications: **. 8**

4.4 Common Operating Platform and Procedures: **. 9**

4.5 Common Operating Procedures during Power Breakdown: **. . . 10**

4.6 Database Environment and Software Development: **. . . . 10**

4.7 Software Support: **. 11**

4.8 Standard Package Application Software: **. 11**

4.9 Integration of Software: **. 11**

5. IT STANDARDS: 12

5.1 After Office hours IT support **. 13**

6. COMMUNICATIONS: 13

6.1 Computer Insurance and Security: **. 13**

7. COMPUTER SECURITY POLICY: 14

7.1 Introduction: **. 14**

7.2 Policy Applicability: **. 16**

7.3 Policy Statements: **. 16**

7.4 Management Responsibility: **. 17**

7.5 Data Owner Responsibilities: **. 18**

7.6 Data User Responsibilities: **18**

7.7 Electronic Mail: **18**

7.8 Auditor Access: **18**

7.9 Unauthorized Software: **19**

7.10 Reporting of Security Problems: **20**

8. APPENDIX “A”:

8.1 Password Management: **20**

8.1.1 Password Selection: **20**

8.1.2 Password Handling:. **21**

9. APPENDIX “B”:

9.1 Disaster Recovery: **22**

9.1.1 Data Backup **22**

9.1.2 Alternate Data Backup **22**

9.1.3 Contingency planning **22**

10. APPENDIX “C”:

10.1 Personnel Security and Security Awareness: **22**

10.1.1 Employee Requirements: **23**

10.1.2 Positions in Sensitive Locations or of Special Trust or Responsibility . . **23**

10.1.3 Security Awareness and Training **23**

10.1.4 Acknowledgment of Rights and Responsibilities: **23**

10.1.5 End of service: **23**

11. APPENDIX “D”:

11.1 Security Policy - Summary Statement: **23**

1. OBJECTIVES:

Information Technology (IT) is, and will be, of great importance to our future development and competitiveness. One critical success factor for the future is to increase the individual's ability to meet future demands for continuous change and improvement and to develop the business process with information technology. Manual information processing cannot meet today's business demands. Computerization will come into more and more areas. It is therefore important to have guidelines and policies which describe the path and lead us towards our long term business objectives to enhance commitment to customers, improve quality of services provided, and increase profitability to develop committed employees.

IT development and operations shall be based on business requirements and it is the responsibility of the manager to ensure that good information systems are applied in his area of responsibility.

IT will be used in order to actively participate in our company's objectives to improve productivity and efficiency in operations, to increase the individual's ability to meet future demands for continuous change and improvement and to ensure effective flow of information, which facilitates cooperation within DEL and external partners.

IT will also enable DEL to take advantage of new opportunities to ensure IT developments with short lead times, adequate quality and security levels and to give DEL an image of being in a premier position with respect to the use of IT.

As recognition of the ever-changing business environment – faster and competitively DEL is placing itself in the best possible position to confront the issues of the twenty-first century.

The future cannot be successfully tackled without the prudent use of Information Technology.

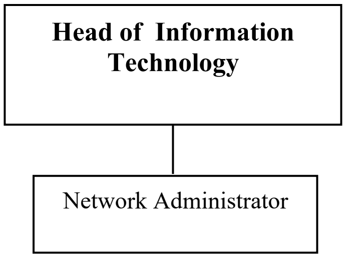
Talal Khan
Head of I.T. - Information Technology
Dawood Equities Limited

2. ORGANIZATION STRUCTURE

IT department reports to Chief Executive Officer. IT Manager participates in determining the strategic direction and operational planning of the business.

Head of I.T. is responsible for providing technical information to the management as well as users for the solutions of their problems. He is also responsible to provide technical services in terms of equipment and manpower to solve systems related problems.

3. IT INFRASTRUCTURE



IT infrastructure consists networks operations, computers hardware, operating systems and communication software. The overall objective with the technical infrastructure is that it shall fulfill the business needs in a cost efficient manner and according to prevailing security and legal requirements.

Business demands on technical structure:

- The user in focus
- Automation support, like word-processing, spreadsheets, presentations and any other application used by the users.
- Electronic mail (E-mail)
- Personnel computers on desktop
- Networks with resource sharing
- Information exchange and interaction, electronic data interchange (EDI)
- Accessibility to the systems on network
- Security in operations, authorization, backups and restoring etc.
- Performance

Other demands:

- Have ability for step by step implementation of the technical infrastructure
- Be based on mainstream products
- Independence between Server products and Client products
- Have flexibility to change and service, not dependent on vendor/supplier
- Reliable vendors/suppliers for the components/parts selected
- Secure and well proven tools
- Follow the legal requirements regarding licenses and copyright laws

4. COMPUTER STANDARDS:

This section describes computer, printer, and network cabling and software standards, which have been, standardized. These standards have been established to minimize long term maintenance costs and support needs. They ensure a high level of systems availability and reliability.

As technology is changing very rapidly, IT is constantly evaluating these standards with new emerging technologies and ideas.

4.1 Computers:

- Server machines shall be based on Intel processors with minimum 8 GB of RAM installed and a large size of Hard Drive.

- Workstations (clients) shall be CORE i7 processor machines with at least 4 GB of RAM to run any future GUI based applications in any heterogeneous computer environment.

- Server machine for corporate office shall be CORE i7 or above with at least 8GB of RAM and shall be on latest Windows 2012 platform.

- Color VGA monitors shall be provided to all Managers and employees. IT reserves the right to install or remove any computer/network equipment from any department for general maintenance and replacement. However, IT shall inform the relevant department heads before installing or removing any computer/network equipment from their department.

- Server machine for Database shall be running Oracle9i Enterprise Edition Release 9.2.0.1.0 Enterprise Server (Developer 2000) on top of Windows Server 2012.

- Server machine shall be at least 8 GB RAM with 17 inches Color Led.

- Workstations shall be at least 4 GB of RAM and 17 inches Color, high resolution led.

- All kinds of file servers, desktop PCs, printer, Notebook PCs etc., shall be specified by IT department. All individual departmental computer/network/software needs shall be evaluated and fulfilled by IT.

- All DEL workstations (clients) shall use Microsoft Windows 10.

- Microsoft Office version 2010 shall be used in conjunction with Windows 10.

Following table specifies the *minimum* configuration all new and upgraded Desktop PCs shall use in office automation.

4.2 IBM Compatible Computer Specifications:

Desktop Machine	
Brand Name	IBM Compatible
Processor, Minimum	Core i7
RAM, Minimum	4 GB
Hard Disk Capacity	250.0 GB Minimum
Universal Flash Drive	32 GB
Network Adapter (NIC)	EtherExpress100BaseT
Modem (If required)	US Robotics 56Kbps
Monitor	LED 17”
Budgetary Pricing	Subjective

4.3 Network Specifications:

Network Standards	
Cable Type	Giga Plus UTP CAT-5 or CAT-6
Cable Manufacturer	AMP, AT&T or Lucent
Switch Specifications	Planet / 3Com / Allied Telesyn
HUB Specifications	3Com
Cabling Topology	STAR
Cable Connectors	RJ-45 AMP/AT&T Brand
Network Adapter (NIC)	EtherExpress100BaseT
Modem	US Robotics 56Kbps / External
Network Protocol	TCP/IP

Budgetary pricing is provided as an indicator only, as pricing varies according to model and specific vendor promotions. At time of purchase a more competitive price may be available.

4.4 Common Operating Platform and Procedures:

Common operating platform shall be heterogeneous i.e. multiple Servers with different operating systems. All Servers shall be connected with each other via TCP/IP protocol and hence will be sharing the same cabling structure.

- The user shall be provided a password for logon. Strict confidentiality must be maintained in supplying passwords. Each user shall be responsible for his/her own password. The group of users specified by Operations and IT shall use any generic password. In case of forgetting the password, the user shall contact IT department immediately. The password shall be maintained as recommended by Risk Management Rules.

- The network cabling scheme shall be structured and shall cater for both voice and data i.e. telephones and computers. 100BaseT, Ethernet, TCP/IP shall be used as local network components.

- Any common users shall not be authorized to modify, reconfigure or relocate any hardware and software equipment. In the case of necessary modifications or reconfigurations, IT personnel shall be informed through “Hardware/Software Maintenance Form”. This form shall be provided by the IT department.

- The user and his department will be responsible for the hardware and software equipment provided by the IT department. This will include hardware like CPU, Monitor, Printer, Mouse, Mouse Pad, connecting cables, computer accessories and all software installed in the computer. The user will be responsible to keep all the hardware clean and tidy at all times.

- All hardware, software and data shall be the property of DEL. Strict confidentiality shall be maintained in transmitting and receiving Company’s data. All users shall maintain this level of confidentiality within and outside the company.

- Strict measures shall be taken in order to prevent data corruption by any means. Virus protection and on-line inoculation software shall be installed in all Servers and workstations. Users shall not be allowed to use any foreign media like Floppies, CDs Zipped Drives or Flash RAMs. In case of emergency, the user may contact IT.

- Care must be taken in switching-on or switching-off any hardware appliance. Each user shall be responsible to Log-out of main Servers before leaving his desk or DEL premises. The operating sequence can be discussed with IT.

4.5 Common Operating Procedures during Power Breakdown:

- All Server room and management computers shall be connected with centralized UPS (Un-interruptable Power System). Flat pin 13A power outlets have been provided for computer equipment only. These outlets shall be connected to UPS. No other electronic or electric appliance shall be connected with these UPS outlets. For special cases, IT may be consulted.

- All Laser printers shall strictly be connected with ordinary, non-UPS 15A power outlets.

- During a power outage, no additional hardware (Computers, Printers, Modems etc.) shall be switched-on. Maximum battery time is 30 minutes and can only be used to perform backup tasks during power outage. All users shall be responsible to save any changes or take backup during this time. All hardware running on UPS shall be switched-off manually or automatically before reaching its maximum backup time.

- In case of fire or other emergencies, all standard safety procedures may be adopted. Safety or IT personnel may also be contacted.

4.6 Database Environment and Software Development:

Dawood Equities limited appoints Vision Max (Pvt.) Limited for developing new applications Oracle9i Enterprise Edition Release 12G or above shall be used as database. can also be used in conjunction with back-end Oracle9i Enterprise Edition Release 9.2.0.1.0 or above database. Before starting a new software development, a series of discussions and meetings shall be required with the relevant department in order to assess and analyze their needs. Standard software development procedures shall be adopted in designing new applications / routines. New application must have User Manuals and analysis report.

The appropriate procedure would be for the concerned department to approach IT about their new software requirements. Meetings for initial briefings and guidelines should be held between the two departments thereafter a potential vendor introduced quotations obtained and software jointly evaluated. During these meetings, Head of the IT Department should take an active role in streamlining discussions, and ensuring proper distribution to relevant personnel afterwards. As a conclusion to these meetings, an action plan should be drawn, responsibility mapped out and budget and implementation approved.

The CEO should be taking an active role also to ensure that continuous progress on this front is being made.

4.7 Software Support

For all kind of software support issues department will contact IT. IT will nominate one administrative user for each application, who will be allowed to contact software vendors in regard to end user related issues only, mentioned correspondence will also be done with the permission of IT Manager.

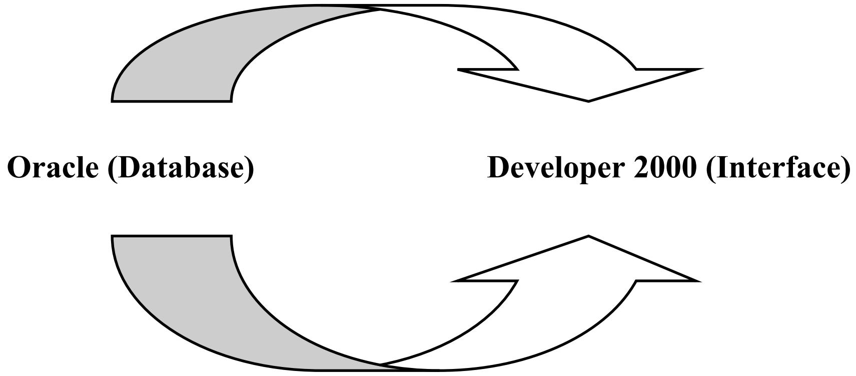
4.8 Standard Package Application Software:

Standardized application software can be purchased off-the-shelf. A standard package must always be treated in the same manner as developed system i.e. it must be fitted into the total systems infrastructure and technical infrastructure and must also be integrated with the present IT environment. For software development, local software developers shall be encouraged. In all such developments, IT shall keep the source codes and copyrights to modify the system in future. All departments shall consult IT prior selecting any software application. IT shall then evaluate the software according to the standard software selection procedures.

4.9 Integration of Software:

Re-key in of data is not always appreciated and IT shall always discourage it. Efforts shall be made to integrate various applications in a secure and efficient manner either by using Windows ODBC or by creating ASCII coded flat files.

Major application, which could be interfaced (linked) together, is:



5. IT STANDARDS:

Some of the reasons for having IT standards:

1. To make cooperation and communication easier within DEL.
2. To give cost efficiency in a total perspective.
3. To make it possible to exchange common solutions between various DEL departments.
4 To make the training and development of users/staff easier.

To conform to the IT standards shall be seen as a goal in a longer perspective. It is not necessary to change everything in a “Big Bang” and rush out and buy new things. We should instead follow the standard whenever we are about to buy or develop something new. This means that we will gradually adopt the standard. If we are about to invest or develop something in a non-standard environment we should always consult with the IT department.

Following list indicates standard hardware and software recommended by IT.

Product Name	Version
UTP Cable	Giga Plus
RJ-45 Connectors	AMP or AT&T
HUB and NIC	Inter Ether Express 100BaseT
Oracle	Oracle9i Enterprise Edition Release 9.2.0.1.0 Developer 2000
Windows Database Server	Server 2012 or above
Trading Interface Server	Server 2012 or above
Feed / Fix Server	Server 2012 or above
Microsoft Windows	Windows 10
Ms Office	Office for Windows 10
Stockxs Client	Stockxs for Windows 10
Vtrade Trading Software	Vtrade for Windows
Database Engine	Oracle RDBMS Oracle9i Enterprise Edition Release 9.2.0.1.0
Internet Software	Microsoft Internet Explorer 11.0 or above
Internet Service Provider	MULTINET / STORM FIBER / WATEEN TELECOM / PTCL
Anti Virus	Symantec

5.1 After Office hours IT support

In case of any emergency Manager may contact designated persons on mentioned telephone # for support.

In case of unavailability designated IT staffs, Manager may also contact IT Head.

6. COMMUNICATIONS:

The E-Mail solution for DEL shall be Microsoft Outlook.

For any additional communication needs, IT shall always be consulted for necessary technical recommendations.

6.1 Computer Insurance and Security:

All hardware and software equipment shall be covered under computer insurance policy. Every department must ensure a sufficient security level regarding:

- **Physical Security:**

  Damage to equipment
  Theft
  Fire

- **Operations Security:**

  Backup
  Power Supply
  Data Integrity
  Virus Control
  Disaster Recovery

- **Information Security:**

  Passwords
  Remote Access by remote logins
  Information Classification

7. COMPUTER SECURITY POLICY:

The ability of DEL to deliver services to its employees and customers has grown enormously through the use of computers. DEL has significant investments in Information Resources. While the value of equipment such as computer hardware is easily appreciated.

Information Resources are vital assets, which require protection. Data, whether stored in central computers accessible through remote terminals, processed locally on microcomputers, or generated by word processing systems, are vulnerable to a variety of threats and must be afforded adequate safeguards.

DEL employees need to be aware of the value of these resources and the means of protecting them. User awareness through education is the first line of defense in maintaining confidentiality, reliability, availability, and integrity of DEL Information Resources.

7.1 Introduction:

Continuing availability of information is essential to the operation of DEL programs. Expanded use of computers and telecommunications has resulted in more accurate, reliable, and faster information processing, with information more readily available to users than ever before. DEL has realized increased productivity, in terms of improved delivery of services, enhanced administrative capabilities, and lower operating costs, as a direct result of the growing commitment to use information technology. Information technology has also brought new administration concerns, challenges, and responsibilities. Information assets must be protected from natural and human hazards. Policies and practices must be established to ensure that hazards are eliminated or their effects minimized.

The focus of information security is on ensuring protection of information and continuation of program operations. Providing efficient accessibility to necessary information is the impetus for establishing and maintaining automated information systems. Protecting that information and the surrounding investment is the impetus for establishing an information security program.

Protecting information assets includes:

- Physical protection of information processing facilities and equipment.
- Maintenance of application and data integrity.
- Assurance that automated information systems perform their critical functions correctly, in a timely manner, and under adequate controls.
- Protection against unauthorized disclosure of information.
- Assurance of the continued availability of reliable and critical information.

Many program operations that traditionally were manual or partially automated are today fully dependent upon the availability of automated information services to perform and support their daily functions. The interruption, disruption, or loss of information support services may adversely affect DEL's ability to administer programs and provide services.

The effects of such risks must be eliminated or minimized.

Additionally, information entered, processed, stored, generated, or disseminated by automated information systems must be protected from internal data or programming errors and from misuse by individuals inside or outside DEL. Specifically, the information must be protected from unauthorized or accidental modification, destruction, or disclosure. Otherwise, we risk compromising the integrity of DEL programs, violating individual rights to privacy, violating copyrights, or facing criminal penalties.

An effective and efficient security management program requires active support and ongoing participation from multiple disciplines and all levels of administration. Responsibilities include identifying vulnerabilities that may affect information assets and implementing cost-effective security practices to minimize or eliminate the effects of the vulnerabilities.

The policies and procedures of this document apply to the mission critical applications and resources operated by DEL IT. In the remainder of this document Information Resources will refer to:

Network Resources - the DEL Computer Network. Departmental LANs are not included except as they are connected to the DEL computer network.

Hardware Resources - all computing resources operated by IT.

Software Resources - all mission critical applications operated by IT for DEL.

7.2 Policy Applicability:

The Computer Security Policy applies to all DEL personnel accessing mission critical applications and computer systems supporting mission critical applications operated by IT.

DEL information security policies and standards apply to Information Resources owned by others, such as state agencies, political subdivisions of the state, or federal government agencies. In the event of a conflict, the more restrictive security measures apply.

7.3 Policy Statements:

It is the policy of DEL that:

Information Resources are valuable assets and unauthorized use, alteration, destruction, or disclosure of these assets is a computer-related crime and punishable.

Attempting to circumvent security or administrative access controls for Information Resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.

Information Resources may be used only for official purposes. Persons using Information Resources will acknowledge compliance with the Computer Security Policy when logon IDs and Passwords are assigned, and in some cases, when an administrative application is accessed. Violations of the Computer Security Policy will be reported to the DEL Chief Executive Officer.

All employees will receive the Computer Security Policy Summary Statement. All new employees will receive a copy from either the Human Resources or Administration Departments. The summary statement is contained in Appendix D, Computer Security Policy Summary Statement. Logon IDs and Passwords must control access to all information Resources. Passwords must be changed periodically by the logon ID owner. All Information Resources used for mission critical applications will require Passwords to be changed maximum every 30 days.

The logon ID owner is responsible to manage their password according to the Guidelines specified in Appendix A, Password Management. The logon ID owner is responsible for all actions and functions performed by their logon ID. Information, which by law is confidential, must be protected from unauthorized access or modification. Data, which is essential to critical functions, must be protected from loss, contamination, or destruction

Confidential information shall be accessible only by personnel who are authorized by the owner on a basis of strict "need to know" in the performance of their duties. Data containing any confidential information shall be readily identifiable and treated as confidential in its entirety.

All Information Resources used for mission critical applications shall have a cost effective, written contingency plan that will provide for prompt and effective continuation of critical missions in the event of a disaster. Appendix B, Disaster Recovery contains additional information.

All employees accessing a mission critical administrative application must receive appropriate training for using the application and must acknowledge the security and privacy requirements for the data contained in the application. Appendix C, Personnel Security and Security Awareness contains additional information.

When an employee terminates employment HR department is required to inform IT, so their access to Information Resources will also be terminated. Appendixes C, Personnel Security and Security Awareness contains additional information.

Microcomputer end-user workstations used in sensitive or critical tasks must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system.

All microcomputer end-user workstations should have virus protection software installed.

Computer software purchased is DEL property and shall be protected as such.

All information processing areas used to house Information Resources supporting mission critical applications must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to these areas shall be restricted to authorized personnel.

Authorized visitors should be supervised and their entry and exit recorded in a log. Internet access to the DEL Network will be directly or indirectly controlled by IT.

7.4 Management Responsibility:

Each Department Head is responsible for the security of information resources in all offices under their jurisdiction and for implementing information security requirements on an office-wide basis.

7.5 Data Owner Responsibilities:

The data owner is responsible for:

- Maintaining the information in the data file.
- Determining how the data may be used within existing policies.
- Authorizing who may access the data.

7.6 Data User Responsibilities:

The data user is the person who has been granted explicit authorization to access the data by the Company. This authorization must be granted according to established procedures.

The user must:

- Use the data only for purposes specified by the Company.
- Comply with security measures specified by the Company or custodian.
- Not disclose information in the data nor the access controls over the data unless specifically authorized in writing by the Company.

7.7 Electronic Mail:

Electronic mail is provided to the employees as part of the Information Resources of DEL to conduct the business of DEL.

Electronic mail is intended to be a convenient way for the employees to communicate for official purpose with one another and colleagues at other locations. It is not the practice of DEL IT to monitor the contents of electronic mail messages. However, the information in electronic mail files may be subject to disclosure under certain circumstances.

7.8 Auditor Access:

There will be occasions when auditors require access to Information Resources and data files. The access will be permitted according to these guidelines:

Internal Auditors from DEL and DEL System:

Personnel of the Internal Audit Departments have access to all activities, records, property, and employees in the performance of their duties.

For non-investigative audits, access requests for Information Resources and data files will be made to the data owner and the administrative management of the organization operating the computers and information resources, as appropriate.

For investigative audits, access requests for Information Resources and data files will be made to the appropriate administrative management level of the organization operating the computers and information resources.

Internal Audit access to data files will be provided as specifically requested by Internal Audit; however, whenever practical, Internal Audit will utilize hard copy output or data file copies. Access is provided to Internal Auditors on all DEL System applications. Read only access will be granted.

All DEL systems including computers, file servers, network components and remote user facilities are governed by the computer security policies which are enforced by the company policy and state laws. Any deviation from these policies may result in disciplinary action (such as cancellation of accounts, dismissal of employment, etc.) and/or legal action (to the extent of relevant law).

The purpose of implementing computer security policy is to minimize the equipment loses, to protect valuable/confidential information and to protect against disasters.

In order to establish and maintain an effective security system within DEL's computing environment a combination of approaches is required:

- A willingness on the part of all users to participate in the security process.

- Participation in the security plan should be perceived as beneficial to everyone, since it assures complete, accurate, timely and secured data.

- A clear set of guidelines which can be used to support the education of the user community.

- A company-wide integration of computer security procedures into normal non-computing office procedures, which deal with the security and integrity of information handled by operational and administrative units of the company.

This policy is freely available to all computer users. All users must read this document so as to be aware of the legal implications and penalties associated with the misuse of the computing facilities and resources.

7.9 Unauthorized Software:

All staff must delete unauthorized software that does not conform to the above guidelines. No user may introduce non-standard software to the DEL systems without approval from the IT or a delegate. A list of authorized software has already been provided to all departmental heads. 'IT reserves the right to unconditionally delete any unauthorized software from any DEL systems.'

7.10 Reporting of Security Problems:

Individuals who wish to report instances of security violations are requested to immediately contact one of the following:

- IT Manager
- Network Administrator

8. APPENDIX “A”

8.1 Password Management

Information handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Effective controls for logical access to information resources minimizes inadvertent employee error and negligence, and reduces opportunities for computer crime. Each user of a mission critical automated system is assigned a unique personal identifier for user identification. User identification is authenticated before the system may grant access to automated information.

8.1.1 Password Selection

Passwords are used to authenticate a user's identity and to establish accountability. A password that is easily guessed is a bad password which compromises security and accountability of actions taken by the logon ID which represents the user's identity.

Now-a-days, computer hackers/crackers are extremely sophisticated. Instead of typing each password by hand, hackers/crackers use personal computers to make phone calls to try the passwords, automatically re-dialing when they become disconnected. Instead of trying every combination of letters, starting with AAAAAA (or whatever), crackers use hit lists of common passwords such as WIZARD or DEMO. Even a modest home computer with a good password guessing program can try thousands of passwords in less than a day's time. Some hit lists used by crackers contain several hundred thousand words. Therefore, any password that anybody might guess to be a password is a bad choice.

What are popular passwords?

Your name, your spouse's name, or your parents' names. Other bad passwords are these names spelled backwards or followed by a single digit. Short passwords are also bad, because there are fewer of them; they are more easily guessed. Especially bad are "magic words" from computer games, such a XYZZY. Other bad choices include phone numbers, characters from favorite movies or books, local landmark names, favorite drinks, or famous people.

Some rules for choosing a good password are:

Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered. Include digits and punctuation characters as well as letters. Choose something easily remembered so it doesn't have to be written down. Use at least 5 characters. Password security is improved slightly by having long passwords. It should be easy to type quickly so someone cannot follow what was typed by watching the keyboard. Use two short words and combine them with a special character or a number, like ROBOT4ME or EYE-CON. Put together an acronym that has special meaning to you, like NOTFSW (None Of This Fancy Stuff Works) or AVPEGCAN (All VAX Programmers Eat Green Cheese At Night).

8.1.2 Password Handling

A standard admonishment is "never write down a password." You should not write your password on your desk calendar, on a Post-It label attached to your computer terminal, or on the pullout drawer of your desk. A password you memorize is more secure than the same password written down, simply because there is less opportunity for other people to learn a memorized password. But a password that must be written down in order to be remembered is quite likely a password that is not going to be guessed easily. If you write a password in your wallet, the chances of somebody who steals your wallet using the password to break into your computer account are remote.

If you must write down a password, follow a few precautions:

Do not identify the password as being a password.

Do not include the name of the account or the phone number of the computer on the same piece of paper.

Do not attach the password to a terminal, keyboard, or any part of a computer.

Mix in some "noise" characters or scramble the written version of the password in a way that you remember, but make the written version different from the real password.

Never record a password on-line and never send a password to another person via electronic mail.

9. APPENDIX “B”

9.1 Disaster Recovery

It is prudent and required by the DEL IT to anticipate and prepare for the loss of information processing capabilities. The plans and actions to recover from losses range from routine backup of data and software in the event of minor losses or temporary outages, to comprehensive disaster recovery planning (as per BCP and DRP) in the preparation for catastrophic losses of information resources.

DEL have a strong backup policy, which is implemented. DEL have a backup server, and it runs a script for backup at 10:00 a. m. every day to take all clients / databases backup. Incase of any disaster we can recovered all our data.

The policy for outside data storage is also mentioned in the attached schedule.

** Schedule of backup is attached.*

9.1.1 Data Backup

On-site backup is employed to have current data readily available in machine-readable form in the production area in the event operating data is lost, damaged, or corrupted; and to avoid having to reenter the data from source material. Off-site backup or storage embodies the same principle but is designed for longer term protection in a more sterile environment, requires less frequent updating, and provides an additional protection against threats potentially damaging to the primary site and data.

Data and software essential to the continued operation of critical department functions must be backed up. The security controls over the backup resources must be as stringent as the protection required of the primary resources.

9.1.2 Alternate Data Backup

The backup procedures on the multi-user computer systems and departmental servers are designed to protect against data losses caused by hardware failures and other disasters. The frequency and timing of these backups may not provide sufficient protection to meet end-user requirements for data backup. Therefore, it is strongly recommended that end-users include a data backup step in their information processing procedures, and not to depend on single backup procedure to provide all protection.

9.1.3 Contingency Planning

Contingency plans, or disaster control plans, specify actions management has approved in advanced to achieve each of three objectives: to identify and respond to disasters; to protect personnel and systems; and to limit damage. The backup plan specifies how to accomplish critical portions of the mission in the absence of a critical resource such as computers. The recovery plan directs recovery of full mission capability.

As DEL have a strong backup policy as well as a “Secondary Domain Server”. Incase of any disaster, we can activate our SDS as Primary Server. These processes take approximately 24 hours to system running smoothly again.

10. APPENDIX “C”

10.1 Personnel Security and Security Awareness

In any organization, people are the greatest asset in maintaining an effective level of security. At the same time, people represent the greatest threats to information security.

No security program can be effective without maintaining employee awareness and motivation.

10.1.1 Employee Requirements

Every employee is responsible for systems security to the degree that the job requires the use of information and associated systems. Fulfillment of security responsibilities is mandatory and violations of security requirements may be cause for disciplinary action, up to and including dismissal, civil penalties, and criminal penalties.

10.1.2 Positions in Sensitive Locations or of Special Trust or Responsibility

Individual positions must be analyzed to determine the potential vulnerabilities associated with work in those positions. In some cases, it may be appropriate for departments, with the approval of the Human Resources Department, to designate classes of employment as being positions of special trust or responsibility. It may also be appropriate to designate locations as sensitive and to require appropriate procedures and safeguards for all employees whose duties include access to those areas.

10.1.3 Security Awareness and Training

An effective level of awareness and training is essential to a viable information security program. Employees who are not informed of risks or of management's policies and interest in security are not likely to take steps to prevent the occurrence of violations. Departments shall provide an ongoing awareness and training program in information security and in the protection of Information Resources for all personnel whose duties bring them into contact with critical or sensitive Company’s Information Resources.

10.1.4 Acknowledgment of Rights and Responsibilities

Employees with access to administrative application systems acknowledge the security requirements of the systems and their responsibility to maintain the security of the systems before access to the system is granted. This acknowledgment occurs by signing the application statement of security responsibility during mandatory training sessions, and by presentation of an on-line statement when the application is accessed.

10.1.5 End of service

HR will inform IT at the end of employee services and accordingly, IT will restrict his access to the network / company applications. Concerned department is required to request IT for data backup otherwise IT will delete employee data/emails after fifteen days.

11. APPENDIX “D”

11.1 Security Policy - Summary Statement

DEL has developed a comprehensive computer security policy statement. This summary statement presents an overview and key points of the DEL Computer Security Policy.

The Information Resources at DEL are extensive and are readily available to authorized users. This availability of computer hardware, software, and database resources brings with it the responsibility to protect those resources from unauthorized access, unauthorized use, or inappropriate use. During the past several years, much has been written about viruses, worms, and hackers. While these are very real and present dangers, we must also be aware of the dangers from careless activities regarding Information Resources at DEL, particularly in the network environment. The DEL Computer Security Policy is available electronically through Internet.

The main items of the Computer Security Policy are:

Each user of an Information Resource must be responsible for certain key aspect of security, which include:

- Appropriate handling of passwords and password procedures.
- Using resources, hardware and software, in accordance with the DEL IT Policies & Guidelines.
- Taking precautions with regard to viruses.
- Following the prescribed procedures for access and use of data.
- Adhering to copyright policies.

DEL has instituted certain computer security measures designed to protect the integrity of Information Resources. Any attempt to circumvent these procedures may be a violation of DEL policies, rules, and regulations. A formal organizational structure has been implemented to monitor computer security at DEL.

DEL do not permit to users’ to use any removable devices. I. T. Department will help to use information extracting from out side from the network domain.

Virus protection software is available and should be installed on all microcomputer end-user workstations and their updates will be sent by IT through Email. Users will be responsible to install these updates in their PCs.

DEL have mounted a very strong firewall onto their Servers (Symantec Antivirus), to secure our Servers and Clients as well.

The policy also clearly defines the owners and users of data within the DEL computing environment. The owners are those persons or offices with responsibility for the collection and maintenance of data. The owner specifies who may use the data, authorizes specific users access to the data, and specifies how the data may be used. Any access to data without the authorization of the data owner is unauthorized use of the data.

FUTURE IMPROVEMENTS

The management will review and may amend or otherwise modify this policy statement from time to time with the approval of Board of Directors of DEL.

BOARD OF DIRECTOR APPROVAL

This policy has been approved by the Board of Directors on 25th day of April 2019.