IT Policy ver1- 2017   
IT Security Policy

# Password policy

All Password must be complex and at least 8 characters includes letters capital and small plus numbers and Special charters   
All Passwords must be changed every 48 days and password history should not reused at least after 3 historical attempts  
No password exchange or expose are allowed for any reason

\*\* Transparent Google and Domain are configured with this policy

# Email policy

Email is only used for business and no unneeded registrations are allowed like social media or other non-business maters   
Communication with non-business individuals is prohibited

PST and OST files is a secondary backup and user is not allowed to remove or delete any of them   
All external Email must be signed and include all sender communication info.

Email must have a backup online in case of any accidental deleting

\*\* Email is now having a backup on another server

# Clean Desk Policy

Leavening any data or devices for long time must be informed by IT Department and all unused devices must be taken to IT Custody

# Data Recovery policy

All Key persons must have 2 backups for their working folders one on their computers and the other on share server in order to backup whole data every day   
minimum retention policy time is 1 day and maximum retention policy time is 1 year

# Antivirus policy

Each computer and server must have company provided antivirus updated and scanning it every day report of the antivirus are monitored and audited by IT department   
Forti Client is our Current Antivirus for Windows MAC and Linux machines

# Data Center Access policy

Data Center is secured by access control each IT personnel have an access card to allow him to enter the Data Center  
In emergency cases IT personnel must provide full detailed report after fixing the issue

Personal devices usage policy   
Personal devices are not welcomed in the company privet network and internet access via company Wi-Fi is prohibited any violation will be monitored and device will be blocked   
  
Leave policy

When any user leaves the company the Company will retrieve all their provided devices and facilities users are not allowed to copy any of their data on external media and this process is supervised by IT personnel's  
User must sign written document from IT as evidence and provide it to HR

IT Support Policy

# Support Process

1. User must send a Ticket on Transparent before any support started
2. The only exception for point one if the user unable to access internet in his/her Room and all other surrounding rooms he/she can call us to support and we will open the ticket for him/her.
3. Remote support is the default way of supporting. IT supporter is not allowed to go personally to fix any problem expect Hardware and physical connections problems.
4. Each type of issue required Certain time to be solved no personnel are allowed to enter IT Room and stay except IT Personals and their superiors.
5. Calls to IT is only supported after sending the ticket
6. External international and home users are not covered.
7. Users have the right to install any applications they needed in work on their own responsibilities. We support only the main applications.
8. Some teams provide support to common applications they need like LE CAT Tools and Software Team Support Development tools and Database as an example.
9. users have the full responsibilities for any data loss we may help them to recover some or move and copy some other but until now we can’t grantee it can be fully backed up.

Support Levels

1. 1st Level of Support Covers (local service and local machines problems and purchasing)
2. 2nd Level of Support Covers (Web Hosting Services Cloud Services Email Services Global internet issues and Backups)
3. 3rd Level of Support Covers (Global Problems and Management related issues)
4. Top Management are the decision makers.

# Support Escalations

1. 1st Level of support is the main support
2. 2nd Level will be involved if 1st level Case exceed its time.
3. 3rd Level will be involved after 1 to 2 Weeks of case exceeding time
4. Top management will be involved after 1 month of case exceeding time

# Local and External Users responsibilities

1. Users have the right to install any applications they needed in work on their own responsibilities.
2. users have the full responsibilities for any data loss we may help them to recover some or move and copy some other but until now we can’t grantee it can be restored.

New Comers processes

1. IT must be notified for the new comer arrival date before at least 7 working days.
2. each new device will need 8 working hours to complete its setup and be ready to deliver included in 7 working days mentioned in point 1
3. if there are any device exchanging approved by managers the time for delivery will be duplicated and additional devices are not included in point 1  
   example if the manger approves to exchange the new laptop with old user and give the old one to the new user time to deliver both is 16 working hours not 8 working hours .
4. creating new comer Emails must be checked and approved by both manager and HR any changes in Email domain location or shape like names or aliases requires 8 working hours (not included in any weekends or public holidays) for delivery and there are no excuses or emergency cases
5. support numbers are updated and from 7:30 AM to 6:30 PM Cairo or +2GMT from Sunday to Thursday    
   Mohamed Esaily 01021110414  
   Ext 1410 VOIP 2005  
   Kamel Abdel Gayed 01092227491

Ext 1039 VOIP 2009  
Emad Hegazy 01092227626

Ext 1441 VOIP 2008

1. External Users are not supported until we approve this policy or modify it for them.

# IT Internet usage policy

# Web applications policy

Only designated web applications are allowed to be used under IT supervision and some are prohibited like  
1- Proxy and tunneling applications

2- P2P applications

3- Cracked applications

4- non business applications like games

# Web usage policy

There are 2 web filtering mechanism used one from UTM and Firewall side and from antivirus side

User is not allowed to bypass any of them and need proper permission if would like to access any additional site you may need a permission from thier Management and IT   
  
IT VPN and External Usage policy

1. VPN Service is a new Feature allowed only to some key persons
2. There are 2 types of VPN one is Remote access and other is web user portal
3. This service is a compliance to our security policy
4. Allowing access to anyone must be approved by their management and IT

Meeting Room Policy

1. Meeting Rooms must be assigned from Transparent
2. All files must be uploaded to [\\meeting-room](file:///\\meeting-room) server
3. Meeting-Room server is the only machine allowed to use the projector.
4. A way of using this server will be shared with HR to distribute it to meeting members.
5. Any change or miss with meeting room equipment must be reported to HR and IT.

Archiving and Backup Policy

Online Servers   
usually it is hosted online and must have a backup and downloaded in scheduled basis daily so we will backup it in additional hard disk and use to download the hard disk contents weekly every weekend and verified every Sunday morning.

Local Servers

I will implement backup management server to check all local server daily and get backup of them

Each server will have its local backup   
Backup Clean up processes on Quarterly basis or Yearly basis "According to backup size " we should take out all old backups to external HDs and free up Room for new backups

Key Persons

Local Key Persons (Managements; PMs and Translators or anyone who kept their data on their computers)

Install a backup agent that can be managed by the management server to take wither full system image or work folder in half day basis 9 AM and 1 PM the full system images will be toked once and kept for safe restoration of data. The location of the full System image will be in their local computers and the work folder will be help in shared privet location.

Freelancers and External key persons

Install the backup agent and monitored by the PM or the key persons themselves as full image daily with version support up to 14 days' versions the backup file should be taken from the key person in every visit.

Audit Policy

# Audit is important to make sure that all processes are in place and working

Internet Audit   
Done by IT and should check any violation of the internet policy above

Security Audit

Done by IT and PMs to insure that all users are comply to the security policy

Backup Audit   
Done by IT for Online servers backup and all in house backups and by PMs and Key persons for all Freelancers home workers and any unreachable persons from IT side.

New Comers check list

Every new comers must be announced to IT before at least 1 week   
IT must follow check list

1. Create all accounts users Email, domain, Transparent any online needed account ie. FTPs.
2. Purchase all missing HW needed for him/her
3. Each user should have PC/Laptop accessorized by Keyboard, mouse, monitor and basic applications last version of Office, Browsers and joining to the domain and connection to internet.
4. for all new products with his/her Give him/her receiving form and training management aid.
5. User must have his/her computer laptop completed and ready to work otherwise he/she must have access to submit a ticket to receive any missing parts.

Backup Process

1. IT will install Backup Agent to all target computers
2. IT Will monitor and Audit successful and fails through Backup management server on daily basis.
3. The Users must report any failure on backups to IT when happens
4. PMs and managers should monitor only their external resources from their daily reports and inform IT for and failure

Audit Process

1. Security Auditing is monitored daily by system admin
2. Each Quarter there is a maintains plan as the following
   1. Check all reported Devices
   2. Reconfigure and fix devices and services
   3. Check with users all current issue and plan any hardware replacements according to budgets and management priorities
   4. Replace bad HW and upgrade any needed to software to newest editions
3. Backup Audit is monitored Via Backup management server through storage admin or system admin and reported to IT Manager daily.