Cognizant
Passion for building stronger businesses

DEFAULT USER RIGHTS ON COGNIZANT NETWORK

The high level guidelines for implementing desktop policy are outlined as follows. The associate is required to go through the below mentioned points and sign the rights document failing which a user id will not be provided:

Physical Access:

Associates shall not be allowed to open or move the Computer System, for any reason.

Desktop BIOS settings:

- **BIOS Setup Password:**
  The BIOS Setup password shall be enforced on all desktop and only known to NSS personnel.
- **Power On /Boot Password:**
  The Power-on password shall be enforced on all desktops. This will serve as a first level access security for the desktops.
- **Booting process:**
  Booting from active devices like CD-ROM, Floppy Drive, Boot ROM etc. shall be disabled.

User Level Access Rights:

- The Associate shall not be a part of the local Administrators / Power Users group. Administrator access shall be removed from the desktop so that the Associate cannot install any software or make any changes to the system settings.
- Associates shall not be permitted to share any folders in their machines.
- Associates shall be advised not to download technical literature / white papers, shareware / freeware software tools etc. from the Internet.
- Associates shall not be allowed to change the basic settings like default IP Address, Service Pack, System Partition, and Default Services etc.

Standard Wallpaper & Screen Saver Implementation:

The standard wallpaper & screen saver [designed by Cognizant] shall be enabled with password protection and an idle timeout of 5 minutes, to prevent unauthorized access.

Operating System Level Security:

To avoid any misuse or unauthorized access, the following OS level restrictions shall be implemented by changing the appropriate registry values:

- Issuance of Anonymous User Accounts shall be restricted.
- Only Administrators shall be allowed to change/configure NT Base objects such as files, printers and processes.
- Only Associates having valid user ID & password shall be allowed to log on to the system.
- Automatic logon shall be disabled.
- Caching of logon credentials shall be disabled.
- Names of previously logged-on users shall not be displayed in order to protect the secrecy of user names.
- Only Administrators shall be allowed to use the scheduler service with the AT Command.
- The NT Page file shall be cleared on system shutdown to prevent a publicized attack to use any information saved on the paging file.

Protecting Floppies and CD-ROM Drives:

Access to floppy disk or CD-ROM Drive shall be restricted to authorized users only.

Remote Access Services:

- Remote Access Services & Dial in Modem port shall be disabled to avoid any possibility of remote access to the desktop from the network.
- Remote access tools like PCAnywhere, VNC, Damewhere etc. shall not be installed on the desktops.

Restricted Access for Shutdown:

Only the currently logged-in user and Administrators can shut down a workstation.

Remote Registry Access:

Remote access to a workstation registry shall be restricted to Administrators only.

Internet Explorer Security Zone Settings:

The IE Security Customization Package, which sets optimized security levels for all security zones and disables users from changing these settings, shall be implemented.

Anti Virus:

Anti-virus software shall be installed on all desktops by default and updated automatically on a regular basis.

Logon Message, Welcome Message and Announcements:

The logon and welcome messages shall not contain any information that could aid unauthorized persons in gaining access to the system.

Name :	Balakrishna P	Date :	9/16/2011

Signed by Balakrishna P
on Sep 16, 2011