**Undertaking for Information Security Compliance to SITA Information and Computing Resources**

**Refs:**

- SITA_Corporate_IT_Policy_NOV 2014.
- Exhibit 'D' to MSA dated 8th October 2007.
- Best Practices & Do's & Don't attached.

I, Emp. ID_____, Name _____ have read and understood the policy document on _____. I recognize and understand that SITA business resources including email/internet is to be used for business purposes only. I understand that the use of SITA facilities for private purposes is strictly prohibited, except when expressly permitted.

I am aware that SITA IT and business may access and review any material created, stored, sent and received by me.

I have read the aforementioned documents and agree to follow all the policies and procedures that are set forth therein. I further agree to abide by the standards set in the documents for the duration of my employment on SITA engagement. I undertake that I shall not misuse the privileged access (Administrative Rights on my machine) granted to me.

I understand that the violation of this undertaking may subject me to disciplinary action up to and including termination from employment, and any legal action in case of illegal act that may be initiated as per Coforge Limited Disciplinary Action Policy.

_____

**Employee Signature**

_____

**Date**

## SUMMARY OF SITA & COFORGE LIMITED SECURITY POLICIES

### Desktop/Laptop Usage

- Users are responsible for the security of their desktops and laptops.
- Users should not install any software or application on their system that is not authorized, or not mandated by the business. All software or application deployment shall be done by IT Support, post obtaining formal approval from respective supervisors.
- Users should ensure that they have enabled boot level password on their laptops/ desktops.
- All necessary patches/hot fixes for the operating system and applications installed should be periodically updated, but not later than 30 days after these are released.
- Users should Log off their system when not working for extended period(s), or whenever the machine is unattended.
- Connecting any device (that are not intended for corporate usage, i.e. engineering or demonstration equipment) to any SITA Corporate or Data Center network without prior authorization from SITA Corporate Desktop is prohibited.

### Anti-Virus

- Users should not disable the installed anti-virus agent, or change its settings.
- Users should check that their anti-virus signatures are being updated at least on a weekly basis.
- Users should not disrupt the automatic virus scan scheduled on their machines.
- All files received from external source(s) should be scanned for virus/ malware before opening.
- Users should report detection of any virus/malware detected in the system and not cleaned by the antivirus, to IT Support. The system should be unplugged from the network immediately.

### Security and Protection of Data

- All PCs, notebooks, laptops, handhelds, mobile devices, workstations, and all other systems or devices which are owned by business and/or that contain company sensitive or confidential information must have a password protected screensaver (or lock feature) which automatically locks the device after no more than 5 minutes of inactivity.
- Users must log off, or manually lock their devices before they leave their systems unattended.
- Important data and documents stored on a workstation must have a backup copy on a SITA-provided file server, a CD or a DVD.

### Use of Passwords

- Users should follow good security practices in the selection and use of passwords. Generally, the following should apply:
  - Passwords should be kept confidential and not shared with anyone.
  - Passwords should not be written down or recorded electronically (e.g. software file, handheld device) unless it is stored securely, and the method of storage has been approved (e.g. Password Safe).
  - Passwords should be changed whenever there is an indication of possible system or password compromise.
  - Passwords should be changed every 30-90 days depending upon system criticality (and avoid re-using or recycling old passwords).

- Select strong passwords which are:
  - A minimum length of eight characters, and include upper and lower case letters, numbers, and special characters.
  - Easy to remember and difficult for other people to guess (i.e. Avoid using date of birth, phone number, name).
  - Do not use plain dictionary words in any language as a password.
  - Do not use consecutive identical characters or all numeric or all alphabetical passwords.

- Do not include passwords in any automated logon process (e.g. stored in a macro or function key). Never use the “remember password” feature on Internet websites.

For more information on password management, please refer to the SITA_Corporate_IT_Policy_November 2014.

**Internet Usage**

- Internet access is provided to users for the performance and fulfilment of job responsibilities.
- Users should access internet only through the connectivity provided by the business and should not set up internet access without authorization from IT Department.
- All access to internet will be authenticated and will be restricted to business related sites.
- Users are responsible for protecting their internet account and password.
- In case of misuse of internet access is detected, business can terminate the user’s internet account and take disciplinary action as business may deem fit.
- Business reserves the right to monitor and review internet usage of users to ensure compliance to the policy.

For more information on internet usage, please refer to the SITA_Corporate_IT_Policy_November 2014

**E-mail Services**

- Use of official mail account for personal purposes is discouraged.
- Users should protect their email account on the server through strong password, and should not share
- their credentials with anyone else.
- Confidential or sensitive information should not be transmitted over email unless it is encrypted or password protected.
- Emails that are not digitally signed should not be used for critical transactions requiring legal authentication of sender.
- Accessing or using an email account assigned to another individual without the owner’s explicit authorization.
- Automatic forwarding of mail intended for SITA email addresses to personal accounts with public or external email providers or any partner company email account.

For more information on email management, please refer to the SITA_Corporate_IT_Policy_November 2014.

**Software Related Controls**

- Users should not Install, remove or modify Corporate Software and configuration of the application without prior authorization from the assets provisioned by SITA.
- Users should not install any Corporate Software or associated components on:
  - Unmanaged computer or hardware asset that is not managed by Corporate Desktop, including contracting staff or personal computers not owned by SITA.
  - A virtual machine environment of any kind.
  - Hardware based outside of the Corporate Desktop supported sites.
  - Hardware located in countries that are specifically excluded from the scope of any or all of the Corporate Software license agreements.
- Users should not Install any software for which proper license ownership allocation cannot be proven by the employee, line or department manager.

**Prohibited Activities**

The following is a list of specific prohibited activities, but this is not exhaustive:

- Using a SITA asset to conduct an activity for inappropriate personal financial gain.
- Violating the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" media that are not appropriately licensed for use by SITA.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, copyrighted music or other copyrighted sources.
- Illegally exporting software, technical information, encryption software, or technology in violation of export control laws.
- Modifying or attempting to modify content on any SITA systems, including the SITA Intranet web site, without prior authorization from the relevant SITA Intranet administrator.
- Loading images, data, or other material of an offensive, obscene, pornographic, or indecent nature on SITA systems.
- Developing or publishing, without the approval of the Senior Vice President, Marketing and Sales Operations, a website that purports to represent SITA.
- Permanently downloading or uploading any materials such as audio, video, or pictures other than for business purposes.
- Procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Any form of harassment via email, messaging, social media, or other communication medium whether through content, frequency, or size of messages.
- Introducing malware (e.g., viruses, worms, Trojan horses, email bombs, etc.) into a SITA network, server, workstation, or any other device or information resource.
- Revealing account passwords to others, or allowing unauthorized use of accounts by others. This includes external individuals such as family and other household members when work is being done at home.
- Circumventing the authentication or security protocols of any host, network, application, or account.
- Effecting security incidents or disruptions of network communication. Security incidents include, but are not limited to, accessing data for which the individual Staff or External Resource is not authorized or logging into a server or account that the individual Staff or External Resource is not expressly authorized to access. "Disruption" includes, but is not limited to, Distributed Denial of Service (DDoS), packet spoofing, denial of service (DoS) attacks, man-in-the-middle attacks (MITM), and forged routing information for malicious purposes.
- Security scanning of SITA networks or systems.
- Installing and/or using software that exhibits hacking-like behaviour on any SITA network or the Internet.
- Using any program, script, command or message of any kind with the intent to interfere with, or disable a member of Staff's or External Resource's terminal session via any means locally or via the Internet/intranet/extranet (i.e. broadcast messages).
- Providing sensitive or confidential information about SITA Staff to parties outside of SITA, including public websites without prior written approval.