**As you are aware we are ISO 27001 certified for information security. As part of the ISMS (Information Security Management Systems)** **there are certain do’s and don’ts that everyone needs to mandatorily follow .Nous as an organization has zero-tolerance to any violation/s of the security and compliance policy. Any deviation would be treated as serious breach of employment terms and appropriate disciplinary actions could be initiated against the person/s immediately.**

**Some attempted cases of violations include:**

**• Emailing or copying source code to personal mail ID’s/personal shared sites**

**• Bypassing configuration management**

**• Emailing project, client artifacts or other official information to personal e-mail ID’s**

**• Disclosing project/ client details/info in resumes/ personal profiles on networking sites**

**• Carrying any undeclared storage devices (Flash drives, USB drives, SD cards) to your work place / connect to your computer**

**• Download / install Freeware/trial software's directly from Internet without the requisite approval from the IT team**

**Every employee should also be aware of the following**

**1. Password Control**

* **Change your domain/Entity passwords regularly, choose a password with a minimum of 8 characters & should be alphanumeric**
* **Your domain user name & password will the same for Active directory and for your email.**
* **Enforce password history 10**
* **Maximum password age 90 days for Domain user login**
* **User will be locked for 3 wrong password attempts**

**2. Guidelines on Use of Camera Phones /Smart phones/Tablets**

* **Personal Camera Phones /Smart phones/Tablets may be permitted in the office but must not be used to collect and store data that belongs to Nous.**
* **Camera Mobile Phones should not be used for taking business related pictures. However, some limited personal use is allowed, depending on the need of some functions, but storage must not interfere with NOUS Business use.**
* **Never attempt to use an unapproved device (iPad /Tablets/Mobiles etc.), via any method of communication, with any IT equipment that belongs to Nous**
* **Personal digital cameras are not allowed to be taken inside the office. However, some limited personal use is allowed, depending on the need of some functions, but storage must not interfere with NOUS Business use. Prior approval from AVP-IT should be taken for such usages.**
* **Inappropriate content is prohibited in camera mobile phones**

**3. Guidelines on use of Bluetooth enabled devices**

* **Bluetooth must only be used for accessing passive devices – such as hands free kits**
* **Bluetooth cannot be used to communicate with a device directly connected to the NOUS data network (unless through a NOUS owned PC)**
* **Never run a NOUS device in broadcast mode, various viruses and other schemes are prevalent whilst in this mode**

**General**

* **Employee’s should always wear the access card & ID card tag. Access cards should not be kept laying unattended**
* **No changes to the security settings or configuration of any approved device can be made without prior authorization from AVP-IT**
* **Don’t carry any storage devices (Floppy, CD’s, Pen drives, USB drives, SD cards) to your work place /connect to your computer.**
* **If you are carrying any personal electronic devices / storage devices while coming to office, it should be declared at the security desk & kept with the security for safe custody. Undeclared items could be subject to data formatting.**

      **Kindly report any event/ incident observed / seen, to** [**secure@nousinfo.com**](mailto:secure@nousinfo.com)