***Q1.***Who **takes responsibility to report** any information security events, incidents, observed or suspected security weaknesses in systems or services to Security Team

A1. Board of management

A2. Security Team

A3. All Staffs

A4. Management Division

**Reference**: [**Information System Security Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Information_System_Security_Policy.aspx), section **3. Responsibility**

***Q2.***To ensure compliance with ISMS, it is the responsibility of each staff member to

A1. Follow instruction of managers

A2. Follow ISMS policies and procedures

A3. Follow instruction of Admin Dept

A4. Follow best practices for IT Security found on Internet.

**Reference**: [**Information System Security Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Information_System_Security_Policy.aspx), section 3**. Responsibility**

***Q3.***ISMS policies and procedures are available to every staff as:

A1. Hard-copy at Admin Dept

A2. Hard-copy at Reception Desk

A3. Hard-copy at IT Dept

A4. Soft-copy on intranet portal

***Q4.***It’s responsibility of repository owners to review users’ access rights to the repository at least every 6 months. After any changes, such as promotion, demotion, or termination of employment, the owner of a repository for a specific project is:

A1. Asset Owner (defined as an individual or entity that has an approved management responsibility for controlling the production, development, maintenance, use and security of the assets)

A2. IT Dept.

A3. QA.

A4. Board of Director.

***Q5.*** Which following statement is correct according to **\_Compliance Policy.docx?**

A. Individuals using systems without authority, or in excess of their authority, are subjected to have all of their activities on the system monitored and recorded by authorized system personnel.

B. Anyone, who is using systems expressly consents to the system monitoring, is advised that if it reveals any evidence of violating to policies, regulation or governmental laws , the evidence will be sent to board of management or law enforcement official.

C. Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

D. Information systems owners shall be responsible for regularly checking their information systems for compliance with security implementation standards:

A1. A,B

A2. B,C

A3. D,A

A4. All.

**Reference:** [**\_ISMS\_Compliance Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Compliance-Policy.aspx), section **4.5.**

***Q6.***According to Acceptable Use Policy, Which option is correct?

A. The data that staff create on the corporate systems remains the property of . Because of the need to protect

network, management cannot guarantee the confidentiality of any information stored on any network device belonging ; authorized individuals within may monitor equipment, systems and network traffic at any time.

B. the data that staff create on the corporate systems remains the property of . Because of the need to protect 's network, management cannot guarantee the confidentiality of any information stored on any network device belonging to . However, authorized individuals within can’t monitor equipment, systems and network traffic at any time without prior agreement from the employee.

C. the data that employees create on the corporate systems is the property of the employee. management cannot guarantee the confidentiality of any information stored on any network device belonging to ; authorized individuals within may monitor equipment, systems and network traffic at any time.

D. the data that employees create on the corporate systems is the property of the employee. management has to guarantee the confidentiality of any information stored on any network device belonging to ; doesn’t have the right to monitor equipment, systems and network traffic.

**Reference**: [**Acceptable Use Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Acceptable_Use_Policy.aspx), section **4.1.**

***Q7.***According to [**Acceptable Use Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Acceptable_Use_Policy.aspx), Which option is **INCORRECT**?

A. Do not leave sensitive or critical information on public shared folders (e.g. [\\Dc04\Public](file:///\\Public)).

B. Do not leave sensitive or critical information on printers.

C. Equipment, information or software should not be taken off-site without prior management authorization.

D. Can share password and account to other.

**Reference**: [**Acceptable Use Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Acceptable_Use_Policy.aspx)**, section 4.2**

***Q8.***Software/OS installed on PCs/Laptops/virtual PC shall be authorized by management, except software on the free pool ([\\192.168.177.122\apps](file:///\\apps) ).If you are required to use a software/OS supplied by customers, you need to

A1. Get approval from Project Manager.

A2. Get approval from Delivery Manager.

A3. Get approval from IT Dept.

A4. Install the software/OS. Approval from customer is enough to use it.

**Reference**: [**Software Control Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Software_Control_Policy.aspx)

***Q9.***Software/OS installed on PCs/Laptops/virtual PC shall be authorized by management, except software on the free pool ([\\192.168.177.122\apps](file:///\\apps). If you are required to use a software/OS to develop the internal tool for , you need to

A1. Get approval from Resource Manager

A2. Get approval from Delivery Manager.

A3. Get approval from IT Dept.

A4. Get approval from Technical Manager.

**Reference**: [**Software Control Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Software_Control_Policy.aspx)

***Q10.*** Software/OS installed on PCs/Laptops shall be authorized by management, except software on the free pool ([\\192.168.177.122\apps](file:///\\apps). If you are required to use a software/OS to research and develop, you need to

A1. Get approval from Resource Manager

A2. Get approval from Delivery Manager.

A3. Get approval from IT Dept.

A4. Get approval from Technical Manager.

**Reference**: [**Software Control Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Software_Control_Policy.aspx)

***Q11.*** Software/OS installed on PCs/Laptops/ virtual PC shall be authorized by management, except software on the free pool ([\\192.168.177.122\apps](file:///\\apps) ). If you want to use a free software/OS found in the Internet. You also notice that the software is listed in the Free Pool, however in an older version. To use this software/OS, you need to

A1. Get approval from Project Manager.

A2. Get approval from Division Manager.

A3. Get approval from IT Dept.

A4. Install the software/OS freely without getting any approval because it’s a free software/OS.

**Reference**: [**Software Control Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Software_Control_Policy.aspx)

***Q12.*** When will Project Manager inform IT to revoke the license of software/OS, if the software/OS licenses are not use anymore?

A1. When the project close.

A2. At 15th monthly

A3. When not use license of Software/OS anymore.

A4. Both A1 and A3

**Reference:** [**Software Control Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Software_Control_Policy.aspx).

***Q13.*** Where repository will store project data/information?

A1. Your Local Machine

A2. On SVN of .

**Reference:** [**Project Repository And File** **Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Project-Repository-And-File_Policy.aspx)

***Q14.*** Who has the right to change (grant or revoke) access rights to a project repository?

A1. Project Manager.

A2. Delivery Manager.

A3. IT Dept.

A4. Repository Owner.

**Reference:** [**Project Repository And File** **Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Project-Repository-And-File_Policy.aspx)

***Q15.*** Transfer Media are any kind of devices or media can store data such as HDD, CDROM, USB Flash Drive, Laptop, PDA, etc. Users are prohibited to plug any transfer media to PCs or network to copy or transfer data in or out without authorization. Who can approve for transfer data in or out in neccessary case?

A1. IT staff.

A2. Team leader.

A3. Project Manager.

A4. Asset Owner (defined as an individual or entity that has an approved management responsibility for controlling the production, development, maintenance, use and security of the assets)

**Reference:** [**Transfer Data Using Media Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Transfer_Data_Using_Media_Policy.aspx), section **6. Policies**

***Q16.*** In FTP/SFTP service, each ftp account has a default quota value of 1 gigabyte (GB). The home folders must not be used as permanent storage. Data files will be deleted automatically to save disk if older than:

A1. 1 week.

A2. 2 weeks.

A3. 1 month.

A4. 2 months.

**Reference:** [**FTP Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_FTP_SFTP_Policy.aspx), section **6. Policies**.

***Q17.*** According to Email Policy, Which option is correct?

A. employees shall have no expectation of privacy in anything they store, send or receive on the company’s e-mail system. IT may monitor email to make sure the sending/receiving email smoothly.

B. employees shall have no expectation of privacy in anything they store, send or receive on the company’s e-mail system. may monitor messages after prior agreement from the employee.

C. shall guarantee privacy in anything the employees store, send or receive on the company’s e-mail system. should not monitor messages.

D. shall guarantee privacy in anything the employees store, send or receive on the company’s e-mail system. should not monitor messages without prior agreement from the employee.

**Reference:** [**Email Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Email_Policy.aspx), section **6. Policies**

***Q18.*** If you are L4-> L6, and you have a mailbox with limitation of 350MB. How much is the limitation of you cannot send mail?

A1. 100MB.

A2. 120MB.

A3. 300MB

A4. 320MB.

**Reference:** [**Email Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Email_Policy.aspx), section **8 Mailbox Size**

***Q19.*** In Printing service, sensitive documents should be removed out of printer immediately. Is it correct?

A1. Yes.

A2. No.

**Reference:** [**Printing Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Printing_Policy.aspx), section **5. Policies**

***Q20.*** Account password will be required to change every:

A1. 1 month

A2. 2 month

A3. 3 month

A4. 6 month

**Reference:** [**Password Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Password_Policy.aspx), section **4. Policies**

***Q21.*** When Guest access to Wireless network, they will be able to access:

A1. Internet

A2. Local Network

A3. Internet + Local Networt

**Reference:** [**Wireless Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Wireless_Policy.aspx), section **6. Policies**

***Q22.*** When **project’s devices** successful accessed to wireless network, they will be able to access:

A1. Internet

A2. Local Network

A3. Project’s network

**Reference:** [**Wireless Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Wireless_Policy.aspx), section **6. Policies**

***Q23.*** Who is got permission to VPN access network from internet?

A1. Project Team leader

A2. User working onsite

A3. User who is approved by PM

A4. User who is approved by Head of Division or higher level

**Reference:** [**VPN Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_VPN_Policy.aspx), section **7. Procedure**

***Q24.*** When users are successfully connected to VPN from internet, they are able to access:

A1. network

A2. Project’s network

A3. network + project’s network

**Reference:** [**VPN Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_VPN_Policy.aspx), section **7. Procedure**

***Q25.*** Is personal laptop connected to network?

A1. Yes

A2. No

**Reference:** [**Laptop Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Laptop_Policy.aspx), section **5.1**

***Q26.*** According to Internet Access Policy, could user able to upload file to internet?

A1. Yes

A2. Just few allowed websites

A3. No

**Reference:** [I**nternet Access Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_-Internet_Access_Policy.aspx), section **6.Policy**

***Q27.*** When user need to download large file (over 50MB) using for work, he/she need to:

A1. Downloading by him/herself.

A2. Downloading with utility tools for faster speed.

A3. Send a request to IT for download support.

**Reference:** [I**nternet Access Policy**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_-Internet_Access_Policy.aspx), section **6** and **7.4**

***Q28.*** According to **PHYSICAL AND ENVIRONMENTAL SECURITY POLICY**, when will we allow to open/unlocked the exterior doors?.

A1. Any time.

A2. While a staff member is in a position to monitor access through the doorway.

A3. Board Director can open the exterior doors any time.

**Reference:** [**PHYSICAL AND ENVIRONMENTAL SECURITY POLICY**](https://intranet.harveynash.vn/helpdeskblog/hvnPAL/Pages/ISMS/HNVN_ISMS_Physical-and-Environmental-Security-Policy.aspx), section 4**.Policy**