Network security policy

Company, name and function:

Date:

Signature:

Please also state "read and approved"

Version	Owner (dept. or function)	Target audience	Approved by	Approval date	Review frequency	Reviewed topics
1	ICT	Employees & Supplier	ICT	07/2023	At least every 3 years	/

I. Introduction

This policy is based on the internationally recognized **ISO standards 27001 on information security and 27002 on information technology** and applies to IT outsourcers or other external suppliers (collectively referred to hereafter as the "User"), who are granted Access to the computer or electronic communications network of VPK Packaging Group NV or one or more of its subsidiaries or affiliates (collectively referred to hereafter as "VPK").

In consideration of VPK granting such Access, User agrees to the terms of this policy.

This policy consists of **3 parts**:

1. **Access control**: obligations User must meet and procedures User must follow to restrict (unauthorized) access to VPK Networks.
2. **During Access**: obligations User must meet and procedures User must follow during Access to VPK Networks.

3. **Miscellaneous**: other provisions concerning information security and information technology, including the notification procedure in case of a network security risk or incident.

The obligations of this policy extend to the authorized employees, contractors and other representatives of User. User must inform all authorized users who will Access VPK Networks of their obligations under this policy, but User remains fully liable for violations towards VPK.

If any User fails to comply with this policy, then such User may, in addition to all other remedies, at the sole discretion of VPK, from that moment onwards, not be eligible to perform services for VPK anymore and/or be denied Access to VPK Networks.

Words with capital letters shall have the meaning as described in title 2.

II. Definitions

- ✓ “Access(ible)” refers to any privilege or authority User may have to view, download, create or modify information on the VPK Network, VPK infrastructure or any other VPK application.

- ✓ “Remote session” refers to any VPK Network Access that is established through a dial-up or continuous connection.

- ✓ “VPK Confidential Information” shall be defined as information that relates to VPK’s past, present and future research, development, business activities, products, services and technical knowledge. VPK Confidential Information includes, but is not limited to, technical and business information relating to VPK’s inventions or products, research and development, production, manufacturing and engineering processes, costs, profit or margin information, employee skills and salaries, finances, customers, marketing, production, future business plans and any third party’s proprietary or confidential information to which User may have Access.

- ✓ “VPK Network(s)” refer(s) to any VPK computer or electronic communications resource or network that processes, stores or transmits VPK data or information, including VPK Confidential Information.

III. What (not) to do

1. ACCESS CONTROL

1.1 In general

User may Access and use VPK Networks only as necessary to further its business or service relationship with VPK. User agrees that it will not otherwise use or Access VPK Networks, for its own use or for any other purpose.

Moreover:

a. User shall only Access VPK Networks and VPK information, including VPK Confidential Information, for which User has been specifically granted Access rights by VPK.
b. User shall not attempt unauthorized access to VPK Networks or allow unauthorized individuals to access VPK's Network, data or information.
c. User shall not access, or attempt to access, any third-party networks or systems by means of the VPK Networks, unless authorized in writing by VPK.
d. The VPK User ID may only be used to log on to VPK Networks and is not meant for use on any other network.
e. User shall not replicate or store VPK information in a way which unnecessarily exposes the information.
f. User shall implement the confidentiality safeguards summarized in Section 2.5.

User shall not input, add, delete or otherwise modify the VPK Networks or data accessible via a VPK Network, except to the extent that User is authorized to do so by VPK in writing.

1.2 Physical and environmental security

User's hardware, such as PC's, workstations and other ICT equipment, which Access a VPK Network:

a. Shall only be physically Accessible by User's authorized employees, contractors and other representatives.

b. Must utilize controls that restrict Access to VPK Networks to only authorized User's employees, contractors and other representatives.
c. Shall not contain any software or remote node connection which allows TCP/IP routing, unless such routing capability is disabled.
d. Shall not utilize a function that automates passwords in the logon process, such as storing a password in a macro, logon script or function key, or checking the "save password" box.
e. Shall be logged-off by User before leaving its computing resources.

1.3 User authentication

VPK's user ID administration. VPK may administer the allocation of individual user IDs to User, in which case User shall provide VPK with:

a. Where practicable, the full name of each individual who will have Access to VPK Networks.
b. Prompt notification, in writing, upon termination of employment or assignment of individuals with Access to VPK Networks, so individual user logon IDs may be changed and other measures may be taken by VPK to prevent unauthorized access.

User's user ID administration. User may be allocated a block of user IDs in which case User is responsible for the management and administration of the user IDs for its operations.

a. User must record the allocation of user IDs in a registry to ensure consistency, avoid duplication and hold individual users accountable for their Access privileges to VPK Network. At VPK's request, User shall provide VPK with a copy of its current and historical VPK user ID registry.
b. As far as practicable, User will take reasonable measures to ensure that a single user ID will not be assigned to multiple users.
c. Upon termination of employment or assignment of individuals with a user ID, User will promptly revoke the user ID for such user.

Authentication credentials. VPK may establish a mechanism for strong authentication credentials, such as, but not limited to, digital certificates, tokens, smartcards and

biometrics to provide Access, accountability and revocation. VPK will, upon establishment of such mechanism, provide User with reasonable notice thereto.

Passwords. Passwords must comply with the following standards:

a. VPK will determine the length of the password or agree on it in case User has to create it.
b. The password must be non-decipherable and non-associative.
c. The password must be changed when the password has been of is suspected of having been made available to an unauthorized user of User or any other third party.
d. The password must be changed at VPK's simple request.

Confidentiality of user IDs and passwords. User acknowledges that any user ID or password granted to User by VPK shall be considered VPK Confidential Information and is only meant for User's exclusive use in connection with its business or service relationship with VPK. User shall encrypt all user IDs and passwords. User will not share, disclose or use in any unauthorized manner VPK granted user IDs and passwords. User is responsible for the actions of any individuals using the user IDs and passwords to access a VPK network. User will indemnify, defend and hold VPK harmless from any demands, claims, actions or causes of actions, losses, damages, costs, expenses, judgements, awards, fines, amounts paid in settlement and other liabilities arising out of User's failure to maintain the security and confidentiality of its users IDs and/or passwords used to Access a VPK Network.

Revocation by VPK. VPK may revoke such IDs and passwords at any time, at VPK's sole discretion, in which case the user ID or password will be deleted.

2. DURING ACCESS

2.1 In general

When accessing a VPK Network, User shall ensure that its own systems and networks are adequately protected from any adverse interaction with the VPK Network and shall ensure that the VPK Network is not undergoing any security risks as a result of User's Access to the VPK Network.

2.2 User's changes to VPK systems

For any changes User makes to VPK's production systems, including but not limited to programs, configuration, or environment, User will:

a. Prior to implementation, fully verify such changes in a test system which replicates the VPK production system,
b. Obtain prior VPK approval and then schedule the change, except on an emergency exception basis, in which case User will notify VPK within twenty-four (24) hours of the change.
c. Supply updated documentation and back out procedures, if pertinent, to VPK at the time of change.
d. Create, maintain, and administer a written change log, including date/time, name of VPK authorization personnel and functional change, which will be available for one year upon request by VPK, within twenty-four (24) hours of such request.

NOTE: if User has a VPK router installed in its premises, the following paragraph does not apply.
User shall create a written log of all VPK Network Access and retain log information for a period of one year.

a. The log shall contain the following information for each remote session: date/time, user ID, first and last name of user, start of call, end of call, purpose, tests performed or actions completed.
b. Such log information shall be available upon request by VPK, within 24 hours of such request.

2.3 Transmission of information to VPK

Encryption. VPK may provide User with an approved encryption mechanism for use in all electronic business transactions with VPK and any electronic sharing of information with VPK. User, upon being provided such mechanism, shall use the VPK approved encryption methodology for all sharing of information with VPK.

Computer viruses. User shall take all reasonable precautions to prevent transmission of a computer virus to VPK Networks and shall maintain current and active anti-virus tools on all computers that will directly interface with VPK Networks. Moreover:

a. User will use anti-virus software to check for and eradicate viruses on all electronic files transmitted to or from VPK.
b. User will notify VPK immediately if a virus is detected in a file sent or received from VPK.

Transmission software. User will use only VPK approved network communication programs for interactions with VPK Networks.

2.4 Software

Protection of software. User may need to use and have Access to: (a) third-party software licensed to VPK and/or (b) VPK proprietary software (referred to collectively as the "Software"). VPK may make available to User such Software upon (i) request by User, (ii) determination by VPK that the use of such Software will serve the business needs of VPK, and (iii) approval by VPK and the third party software licensor. If VPK makes such Software available, User will:

a. Use third-party software in strict accordance with all terms and conditions imposed by the software licensor.
b. Use the Software only for the purpose of furthering the business or service relationship with VPK.
c. Not copy the Software, except for VPK authorized back-ups.
d. Treat the Software as VPK Confidential Information.
e. Upon completion of services under this Agreement, return the Software to VPK, if applicable, or destroy all copies of the Software in its possession.

Third party agreements. User's use of third-party software may require User to sign a confidentiality agreement and/or a software license agreement for such software (collectively "Third Party Agreements"). User will sign and execute such Third Party Agreements on VPK's reasonable request and the parties shall mutually agree on which party is responsible for the payment of third party software license fees, if applicable.

2.5 VPK Confidential Information

User acknowledges that information disclosed to it by VPK, or to which User will otherwise have Access via a VPK Network, may include VPK Confidential Information. User agrees that it will use such information only as necessary to further its business or

service relationship with VPK and that it will not otherwise appropriate such information for its own use or for the use of third parties.

User agrees to protect the confidentiality of the VPK Confidential Information in the same manner that it protects the confidentiality of its own confidential information. Where applicable, User shall apply the following precautions:

- Label all print-outs or tangible materials incorporating VPK Confidential Information with the classification 'VPK Confidential'.
- Treat the VPK Confidential Information as sensitive and protect it from unauthorized use or disclosure.
- Restrict disclosure of VPK Confidential Information solely to its employees and contractors with a need to know based on User's business or service relationship with VPK.
- Inform every employee and contractor of User of the existence of this confidentiality obligation.
- Physically secure work areas and materials containing VPK Confidential Information.
- Dispose of hard copy or tangible materials containing VPK Confidential Information in a shredder or a confidential trash disposal bin.
- "Wipe" all magnetic or electronic storage media, prior to discard or reissue, to make any VPK Confidential Information unrecoverable.
- Treat all information on VPK network addresses as VPK Confidential Information, which includes, but is not limited to, not publishing the information on any external networks.

Information shall not be considered VPK Confidential Information if (1) it has been published or is otherwise readily available to the public other than by breach of this Agreement; (2) it has been rightfully received by recipient from a third party without confidentiality limitations; (3) it has been independently developed for recipient by personnel or agents having no Access to VPK Confidential Information; or (4) it was known to recipient prior to its first receipt from the discloser. In the event the recipient receives a subpoena or other validly issued administrative or judicial process requesting VPK Confidential Information (the "Subpoena"), it shall provide prompt notice to VPK of such receipt. The party receiving the Subpoena shall thereafter be entitled to comply with such Subpoena or other process to the extent permitted by law, but shall make

reasonable efforts to maintain the confidentiality of the VPK Confidential Information disclosed under the Subpoena, to the extent legally permitted.

3. MISCELLANEOUS

3.1 Audit and monitoring

User, while Accessing VPK Networks, may have its use of such network monitored and recorded by VPK or a service provider of VPK. User expressly consents to such monitoring and recording.

VPK may, upon reasonable notice, audit User's compliance with confidentiality and security requirements in this policy. Upon notice to User, VPK will have the right to visit User's site during ordinary business hours to review User's security measures and controls.

3.2 Network security risks and incidents

User shall notify VPK immediately of any security risk or breach concerning the VPK Network or any security risk or breach concerning its own network which may adversely affect the VPK Network. By way of example, if User discovers that its network has been affected by a virus, User must immediately notify VPK. In addition, if User becomes aware of a violation of VPK Confidential Information, User must notify VPK immediately. In the event of a network security risk or breach, User agrees to terminate Access to VPK Networks until VPK has re-authorized User to Access such VPK Networks. In addition, User shall cooperate fully with VPK to protect the VPK Network(s) and information and will report to VPK any suspected inadequacy of physical or electronic communications security.

3.3 Intellectual property

User may not use or alter the name, trademarks or other intellectual property belonging to VPK, or to a third party but accessed via a VPK Network, except as specifically authorized in writing by VPK.

3.4 Return of information

User agrees that it will, upon request of VPK and at the sole discretion of VPK, either (i) return to VPK or (ii) destroy all materials containing VPK information, including VPK Confidential Information. VPK may further require that User certifies in writing that it has fulfilled its obligations under this provision.