Non-binding publication of the German Insurance Association (GDV)
for facultative use. Other conditions may be agreed.
In case of deviations, only the German wording shall be binding and prevail.

DTV Terms & Conditions of Liability Insurance for Open-Cover Policies of Carriers, Freight Forwarders and Warehouse Operators 2003/2011

(DTV-VHV Open Policy 2003/2011)

– Explanatory notes on Clause 7.1.5 (Last Amendment: November 2017) –

Sample terms and conditions of the GDV

The following notes contain sample measures for protecting and safeguarding information processing systems. It is incumbent on the Insured to decide specifically how these individual measures are to be implemented, under due consideration of the size of the company and the scope of IT deployment. This can equally mean, that additional measures or more expansive measures may be required in order to comply with the obligation under Clause 7.1.5.

Protection against unauthorised access

Information processing systems must be able to discriminate between different users and levels of authority. Therefore, individual access rights must be defined for all users and these must be adequately secured by passwords comprising, where possible, a mixture of both upper and lower-case letters, numbers, and special characters. Administrative access rights are reserved exclusively for administrators and their respective duties.

These rights must be furnished with additional protection against unauthorised access whenever they are subject to an increased risk. An increased risk can be deemed for devices that are accessible via the Internet or in mobile usage.
Additional protective measures can include, for example: a firewall, 2-factor authentication on servers, encryption of the data carriers of mobile devices, theft protection or similar effective measures.

Anti-malware protection with automatic updates is also required (e.g. a virus scanner, code signing, an application firewall or similar effective measures).

Backing up and protecting data

Systems must be subject to a patch management procedure to ensure that relevant security patches are installed promptly. Systems and applications with known security flaws must not be used unless additional security measures for protection have been implemented.

Unless otherwise agreed, systems must be backed up at least once a week and the respective backup data carrier is to be physically separated to ensure that in the event of a loss or damage the original and duplicate data cannot be accessed simultaneously or that these cannot be manipulated or destroyed.

Systems must be adequately protected against damage or malfunction by authorised users, for example by introducing policies governing the private use and deployment of data carriers and software, and by organising training courses on IT security.

Ongoing checks

The Insured shall carry out checks at regular intervals to ensure that process for backing up and restoring data functions correctly.

State of the art

Deployed systems must correspond to the latest technical standards, be maintained in their latest versions, and be authorised for commercial use.

The Insured shall comply with the obligation under Clause 7.1.5 even where external providers are appointed to carry out work.