

Pier

Country Annex — United States

Vendor statement of facts relevant to local requirements

Document ID	IM.PIER.US.A1
Document version	1.0
Date of issue	2026-10-06
Applies to	Pier 0.3.1
Language	English
Publisher	iMobile

Contents

- 1. Purpose and status 3
- 2. Product facts 3
 - 2.1. Personal data the product can process 3
 - 2.2. Where data is stored 4
 - 2.3. Data sent to the vendor 4
- 3. Privacy 4
 - 3.1. Roles 4
 - 3.2. What the product provides 5
 - 3.3. What remains with the customer 5
- 4. Accessibility 5
- 5. Software supply chain 6
- 6. Cryptography and export controls 6
- 7. Government contracts 7
- 8. Language 7
- 9. Documents usually requested and where to find them 7

About this document

This annex supplements the documentation of Pier version 0.3.1 for customers in the United States. It sets out the facts about the product that matter under the local rules named below and shows which obligations stay with the customer.

The annex is a statement by the vendor about its product. It is not legal advice, not a certificate of conformity and not a substitute for the customer's own assessment.

1. Purpose and status

No certification, authorisation or registration by United States federal or state authorities is claimed for the product or for the vendor in this document.

2. Product facts

Item	Fact
Product and version	Pier 0.3.1
Deployment	Desktop software installed on the customer's computers
Customer content on vendor servers	No
Interface languages	English, Russian, German, French, Spanish, Italian, Portuguese (Brazil), Polish, Turkish, Arabic, Persian, Chinese (Simplified), Japanese, Korean, Vietnamese and Indonesian, 16 in total. The language follows the Windows settings or is chosen on the Settings tab. Error messages of the service, command-line output and log records are in English.

2.1. Personal data the product can process

- The e-mail address of the person who registers the product (sent to the vendor's account server)
- A computer identifier computed as a hash of the Windows MachineGuid, and the computer's network address as seen by the vendor's server when it is contacted
- Credentials for the customer's storage servers: logins, passwords, SSH private keys, S3 access keys (stored on the customer's computer only)
- The content and names of files on mounted drives and in backups, which is whatever the customer keeps there, personal data included (processed on the customer's computer and sent only to the storage servers the customer configures)
- Server names, logins and file paths in the product's local logs

2.2. Where data is stored

The product's data is kept on the customer's computer. In `%ProgramData%\Pier:` the file `config.json` with the settings and drives (passwords and keys under DPAPI protection), the folder `cache` with the block cache of files and the queue of unsent changes (the cache location is configurable), the folder `backup` with the backup jobs, the state of the last run and the job logs (accessible to SYSTEM and administrators only), the files `install.json` (date of the first start) and `license.json` (signed edition terms), the folder `update` with downloaded update files, and the logs `service.log`, `update.log` and `setup.log`. In the user's `%LOCALAPPDATA%\Pier:` the file `account.json` (e-mail address, account token under DPAPI protection, edition terms), the folder `ads` (ad pictures) and the log `tray.log`. Files of mounted drives and backups are kept on the servers the customer configures. File content and names, storage addresses, logins, passwords and keys are not sent to the vendor. The product has no telemetry and no crash reporting.

2.3. Data sent to the vendor

- Request for a registration code: e-mail address, product identifier, interface language
- Activation: e-mail address, the code from the e-mail, product identifier, computer identifier
- Fetching the edition terms when the product's icon starts, once an hour while it runs and on the Refresh license button: account token, product identifier, product version, interface language, computer identifier
- Update check by the service 90 seconds after it starts, every 6 hours and on command: product identifier and product version, followed by the download of the new version's file when there is one
- In the Free edition when ads are shown: download of the ad pictures, and reports that an ad was shown or clicked (token, product identifier, event type, ad identifier)
- Download of the Dokany driver installer from the vendor's website when the driver is missing and the user agreed to install it, or when an update being installed needs it

3. Privacy

The United States has no single federal privacy statute for the private sector. Contracts most often refer to the state consumer-privacy laws, above all the California Consumer Privacy Act as amended by the CPRA (Cal. Civ. Code § 1798.100 et seq.), and to sector laws.

3.1. Roles

For personal data processed in the product on the customer's own equipment, the customer is the business (the CCPA term; "controller" in other state laws). The vendor has no access to that data and is not a service provider for it.

For the data listed under "Data sent to the vendor", which the vendor receives in order to perform the licence agreement, the vendor is itself a business (the CCPA term; "controller" in other state laws).

3.2. What the product provides

- **Access control.** The product has no user accounts or sign-in of its own. It accesses a storage server as the server account set in the drive's configuration (login and password, SSH key, uid and gid values for NFS, S3 access keys); the product performs no multi-factor authentication. A mounted drive is available to every user of the computer with full rights at the Windows level, while the rights on the server are those of the account configured for the drive. Any user signed in on the computer can add, change, mount and remove drives: the service's local control channel is open to authenticated users, and connections to it from other computers are rejected. The service performs backup operations only for members of the local Administrators group; a restore writes files with the rights of the user who requested it. Installation and removal require administrator rights. The account with the vendor is confirmed by a one-time code sent by e-mail.
- **Logging.** The service keeps a text log, `%ProgramData%\Pier\service.log`: start and stop, results of server checks, mounts, errors, file uploads with their paths, update checks and edition terms. At 4 MB the file is renamed to `service.log.1` and the previous `service.log.1` is deleted. Separate logs: `update.log` and `setup.log` in the same folder, `tray.log` in `%LOCALAPPDATA%\Pier`, and a `log.txt` for each backup job under `%ProgramData%\Pier\backup` (up to 1 MB, after which the older half is dropped). There is no record of user actions that says who performed an operation. The product does not write to the Windows event log and does not forward logs to external systems.
- **Export and deletion.** Files on mounted drives remain ordinary files on the customer's servers and can be reached with any client of the same protocol, without Pier. Backups are kept in the product's own format and can be read only by Pier with the backup password; data is taken out of them by restoring the required version to a folder. Settings are kept in JSON files. Removing a drive in the settings window deletes its cache together with any unsent changes. Backup versions are deleted in the restore window or with the commands `Pier.exe backup forget` and `Pier.exe backup prune`, and a whole backup by deleting its folder on the server. After the product is uninstalled, the folders `%ProgramData%\Pier` and `%LOCALAPPDATA%\Pier` are deleted by hand. The product has no function for deleting the registration data held by the vendor's account server.
- **Encryption.** See the section on cryptography below.

3.3. What remains with the customer

- the notice at collection and the privacy policy;
- answering consumer requests to know, delete and correct, using the export and deletion functions above;
- deciding whether regulated categories of data may be placed in the product. No assessment of the product against HIPAA, GLBA, FERPA, COPPA or PCI DSS is claimed in this document.

4. Accessibility

Federal agencies, and many state bodies and universities, buy information technology against Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), whose standards incorporate WCAG 2.0 Level AA, and ask the vendor for an Accessibility Conformance Report on the VPAT template.

Status of the product: No accessibility conformance assessment has been carried out. The interface is built from standard Windows controls: controls can be reached from the keyboard and are exposed through UI Automation (the automated interface tests rely on this), windows scale with the display settings (Per-Monitor DPI v2), and right-to-left layout is used for Arabic and Persian.

No Accessibility Conformance Report (VPAT) is provided for this version.

5. Software supply chain

Federal agencies set their own software-assurance requirements (OMB Memorandum M-26-05). An agency may ask a software producer for a statement on secure development practices aligned with the NIST Secure Software Development Framework (NIST SP 800-218) and for a software bill of materials (SBOM).

- Development and release practices are described in "Software Lifecycle, Maintenance and Support".
- Third-party components and their licences are listed in "Delivery Specification and Third-Party Components". The list is human-readable; no SBOM in SPDX or CycloneDX format is provided for this version.
- No secure-development attestation is provided for this version.

6. Cryptography and export controls

The product uses cryptography as follows:

- WebDAV and S3 channels: HTTPS provided by Windows (WinHTTP, Schannel). The product enables TLS 1.2 and TLS 1.3, and the actual version and cipher suite are decided by the operating system and the server. The server certificate is validated against the Windows certificate store, and validation can be switched off in the drive settings. Plain HTTP without encryption is possible when the user configures it
- WebDAV authentication: HTTP Basic (login and password in the request header) or, when the server demands it, Negotiate, NTLM or Digest through WinHTTP. S3 requests are signed with AWS Signature Version 4 (HMAC-SHA256, SHA-256 payload hash)
- SFTP channel: the SSH-2 protocol, the libssh2 1.11.1 library with Windows CNG for cryptographic operations. Key exchange: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1, diffie-hellman-group-exchange-sha1. Host keys: ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256, ssh-rsa. Ciphers: chacha20-poly1305@openssh.com, aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, arcfour128, arcfour, 3des-cbc. MACs: hmac-sha2-256, hmac-sha2-512 (also in encrypt-then-MAC mode), hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96. Algorithms are chosen by negotiation with the server. The product does not verify or remember the server's host key
- SFTP authentication: password, keyboard-interactive, or the user's private key of type RSA, ECDSA (nistp256, nistp384, nistp521) or Ed25519. Ed25519 signatures are made by built-in code derived from TweetNaCl, RSA and ECDSA signatures by Windows CNG. OpenSSH-format keys protected by a passphrase are decrypted with bcrypt-pbkdf and AES-256-CTR
- NFS version 3: no encryption and no cryptographic authentication (AUTH_SYS)
- Pier Backup copies are encrypted on the computer before they are sent: AES-256-GCM (Windows CNG), a random 96-bit nonce per block, a 128-bit authentication tag. The 256-bit encryption key and the 256-bit identifier key are produced by the Windows random number generator and written to the backup repository encrypted under a key derived from the backup password with PBKDF2-HMAC-SHA256 (600,000 iterations, 256-bit salt). Block identifiers are HMAC-SHA256 values, and repository file names are the SHA-256 of their content

- Secrets on the computer: passwords and private keys of drives and backup jobs are protected with Windows DPAPI bound to the computer, the account token with DPAPI bound to the Windows user. The block cache of files on the local disk is not encrypted
- Exchange with the vendor's account server: HTTPS provided by Windows (WinHTTP, Schannel), TLS versions as configured in the operating system. Edition terms and update information are signed with ECDSA P-256 and SHA-256 and verified with a built-in public key. The update file and the driver installer are checked by SHA-256
- The product has not been validated under FIPS 140-3. Where the list above names cryptographic services of the operating system, their validation status is that of the operating system.
- The product is developed and published outside the United States. No U.S. export classification (ECCN) is claimed for it. A customer that exports or re-exports the product from the United States determines its own obligations under the Export Administration Regulations (15 C.F.R. Parts 730–774).

7. Government contracts

- **Rights in software.** The software and its documentation are "commercial computer software" and "commercial computer software documentation" within the meaning of Part 12 of the Federal Acquisition Regulation and DFARS 227.7202. U.S. Government end users acquire them with only the rights set out in the vendor's licence agreement.
- **Country of origin.** A statement for the purposes of the Trade Agreements Act (19 U.S.C. § 2501 et seq.; FAR 52.225-5) depends on the contracting entity and is given in the contract; none is made here.

8. Language

This package is supplied in English. This annex is laid out for US Letter paper; the other documents of the package are laid out for A4.

Interface languages of the product: English, Russian, German, French, Spanish, Italian, Portuguese (Brazil), Polish, Turkish, Arabic, Persian, Chinese (Simplified), Japanese, Korean, Vietnamese and Indonesian, 16 in total. The language follows the Windows settings or is chosen on the Settings tab. Error messages of the service, command-line output and log records are in English.

9. Documents usually requested and where to find them

Usually requested	Where it is
Product description, functional specification	Product Description and Functional Specification
Installation and operating instructions	Installation and Administration Guide
User manual	User Guide
Maintenance and support description	Software Lifecycle, Maintenance and Support. Service levels: contract
List of third-party and open-source components	Delivery Specification and Third-Party Components
Security and data-protection description	Security and Data Protection Statement

Usually requested	Where it is
Accessibility Conformance Report (VPAT)	Not provided for this version
SBOM (SPDX or CycloneDX), secure-development attestation	Not provided for this version; component list as above
Service-provider terms (CCPA), business associate agreement (HIPAA)	Contract, where applicable
Licence agreement, warranties, prices	Contract

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	0.3.1	First issue