Data Protection Policy

Hague Australia (HAGUE) is committed to meeting its obligations under the Commonwealth Privacy Act 1988 and Telecommunications Act 1997. HAGUE will strive to observe the law in all collection and processing of subject data and will meet any subject access request in compliance with the law. HAGUE will only use data in ways relevant to carrying out its legitimate purposes and functions as a company in a way that is not prejudicial to the interests of individuals.

HAGUE will take due care in the collection and storage of any sensitive data. HAGUE staff will do their utmost to keep all data accurate, timely and secure.

As an Australian registered company, HAGUE may share its data with HAGUE staff, clients, suppliers and partners but will work to ensure that all staff understand they are required to observe data protection laws.

All HAGUE staff, whether permanent or temporary, and voluntary workers, must be aware of the requirements of the Commonwealth Privacy Act when they collect or handle data about an individual.

HAGUE staff must not disclose data except where there is subject consent, or legal requirement. Data sent to outside agencies must always be protected by a written contract. All collection and processing must be done in good faith.

The Data Protection Desk will keep records of all complaints by data subjects and the follow up. It will also keep a record of all data access requests. There will be a repository of all HAGUE statements of Data Protection Law compliance and information about any contacts made with the Data Protection Registrar. This information will be available to staff and data subjects on request.

HAGUE will inform subjects of any processing, disclosure or overseas transfer that does not fall within HAGUE's purpose in a way that any individual supplying could be expected to understand. HAGUE will keep registration (now called notification) up to date.

Data Protection Policy

Data Protection

The principles have been defined to ensure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights Secure
- Not transferred to other countries without adequate protection

The Customer agrees that HAGUE will hold a level of responsibility under the Commonwealth Privacy Act 1998 that is appropriate to the level of understanding that it has been granted in its role as a contracted data processor.

The Customer will be responsible for ensuring that the eight data protection principles are followed in relation to whoever has designed the business purpose of the project and performed the role of the data collector.

Data Exchange Methods

We recognise that our Customers and, as applicable, their nominated agents have a range of capabilities when exchanging data and we are keen to help you select a method that suits your requirements. The options for data exchange outlined overleaf are covered by this Standard Agreement and have been designed to be robust and to balance flexibility and security needs.

If your requirements are not covered by our standard procedures, we will be happy to discuss them with you, however, this may require that a separate agreement be drawn up and co-signed.

Data Protection Policy

Standard Data Exchange Methods:

Option 1: You send data to our Secure FTP site (SFTP)

- We use Active Directory Authentication and log all connections to the sites.
- Usernames and password are communicated by different methods.
- Data Upload:
    - Every customer has a separate secure upload location We block a specific list of potentially dangerous file types
- Data Download:
    - Every customer has a separate secure download location
    - Separate documents are available giving more details of our SFTP services. These are available on request.

Option 2: You email data files to us as attachments

- We have an email address that is specifically used for automating the transfer of data files. This is a not an individual's address as we prefer to avoid storing sensitive data in an individual's email account.
- Sender address' must be registered with us before data files can be sent to this address. Email from unrecognised senders is automatically deleted.
- Nominated HAGUE staff are notified once files are accepted. Files are automatically stripped out and saved to a secure customer specific folder Notification of receipt of data is returned to the sender, once data has been accepted. All mails to this address are logged.
- All mails are scanned for viruses.
- Potentially dangerous file types are blocked.
- A separate document is available giving more details of our 'filetransfer' email address.

Option 3: We collect data from your SFTP site

- We can retrieve files from client FTP and SFTP sites
- We advise that the precautions outlined in the 'security of data in transit' section overleaf are used to protect any data made available to us via your own FTP sites.

Data Protection Policy

Data Access

As a matter of principal, we prefer to automate the exchange of data. Our reasoning is that if the Customer or, as applicable, their nominated agent controls the transfer, the process will run more smoothly than if HAGUE must react at specific times to manually collect data.

As a result, we strongly recommend data exchange option 1, followed by option 2. Options 3 is available, but this is more difficult for us to manage and audit.

Immediately a file arrives on our SFTP server (option 1) it will automatically be replicated to a specifically named customer folder on our primary server, this is mirrored to our failover server. A similar automated process replicates emailed files (option 2) to the relevant customer folder.

When a Customer or their nominated agent is granted access rights to HAGUE SFTP site (option 1), they will be assigned one or more user access accounts, each will be associated with a username and password. The Customer must ensure that these access credentials are tightly controlled and are only available to authorised persons. If the Customer believes that the credentials are in the possession of an unauthorised person, including anyone who may have left their or their agents' business, they should inform their HAGUE account manager immediately to arrange the account to be disabled or the password reset as appropriate. HAGUE will not accept liability for data loss or unauthorised access in the event of uncontrolled credentials.

If we are required to collect data from your SFTP site (option 3), HAGUE staff will save the files to the same customer specific folders as described above.

The servers are located in a locked and intruder alarmed area within HAGUE access-controlled site.

Access rights to the Customer data folders are allocated only to those HAGUE staff that need access in order to support production. Typically, this will be the relevant customer service and programming staff. The assignment of access rights is strictly controlled and audited though our ISO27001 information security procedures, where authorisation must be received in writing from one of two designated senior managers before access is granted. Authorisations are retained for audit purposes.

To reduce the risk of data loss and unauthorised access, our policy is that sensitive data may only be held on HAGUE servers; the storage of sensitive data on desktop PCs, laptops or other mobile devices (portable drives, USB memory keys, CDs etc.) is forbidden. For this reason, we discourage

the exchange of data using physical media and the sending of files to the email accounts of HAGUE staff. Whilst we understand that some customers may choose to deliver data in this way, these methods have a greater level of risk, irrespective of whether the data is encrypted or not, and are excluded from the scope of this agreement. Our acceptance and processing of data delivered by these methods is on the understanding that the customer accepts all liability for data loss and unauthorised access.

HAGUE has formal policies and procedures to manage the disposal of redundant equipment and the safe destruction of physical media.

Data Retention

This Standard Agreement provides for data to be retained on HAGUE servers for a period of 90 days from receipt, after this the files will be deleted by an automated script which is run each day. If you require a different retention period, please advise your HAGUE account manager in writing.

Data Protection Policy

Security of Data in Transit

HAGUE and the Customer undertake within this Standard Agreement that:

1. All sensitive data will be encrypted before being placed in transit. If the Customer is unfamiliar with data encryption HAGUE can provide a guide which gives a brief outline of how different types of encryption work. This can be requested from the relevant Customer Services Account Manager at HAGUE.
2. Note: Sensitive data can be encrypted, zipped and password protected using programs such as WinZip, SecureZip, SevenZip and PGPZip.
3. Passwords must be at least 8 characters in length and contain a mix of upper and lower case characters as well as digits and special characters (%#!@?>}|\).

Passwords must not be sent at the same time as the data itself. For example, if the Customer or their nominated agent emails a password protected zip file to HAGUE data exchange address, they must not include the password in the same communication. The password must either be agreed prior to the exchange of data or sent in a separate email to their designated contact at HAGUE.

HAGUE staff will follow the same principles for ensuring the security of data in transit if there is a requirement to transfer sensitive data to Customers.

Data Leakage

In the absence of any separate co-signed agreement, the Customer accepts that this Standard Agreement has primacy and that the principles described to guard against data loss and unauthorised access are understood and will be applied.

The Customer takes full responsibility for data loss and unauthorised access should any unencrypted file that they send to HAGUE come into the public domain. In this situation the Customer absolves HAGUE from any liability or associated legal action that may be associated with any instance of data loss or unauthorised access associated with an unsecured file.

System Availability and Support

HAGUE will endeavor to provide, but cannot guarantee, the infrastructure and services to exchange data with customers 24/7.

Customers who require technical or other support should contact their normal Customer Services Account Manager between 09:00 and 16:00 Monday to Friday (excluding Public Holidays)