OUR CYBERSECURITY APPROACH

At U.S. Xpress, we organize cybersecurity in eight domains.

1. Security and risk management

U.S. Xpress has a set of IT (Information Technology) security policies that all employees are expected to comply with. Regular cybersecurity training is conducted for all employees. Various contingency plans are on file and training is conducted regularly.

2. Asset security

U.S. Xpress secures and monitors devices to protect confidentiality of information. Assets are covered by policies that describe proper use, and disposal to prevent unauthorized disclosure of information.

3. Security architecture and engineering

U.S. Xpress has a vulnerability management program that regularly checks for and remediates vulnerabilities. Secure protocols and components are used to develop information systems.

4. Communication and network security

U.S. Xpress uses encryption protocols that protect data at rest and in transit. The network and devices are monitored for threats to the systems.

5. Identity and access management

U.S. Xpress controls access to information systems to limit access and monitor system usage. Where appropriate, we use additional measures to control logical and physical access to the systems and physical sites.

6. Security testing and assessments

U.S. Xpress conducts regular third-party assessments to evaluate our security posture. Penetration tests are regularly conducted by a third party to assess the effectiveness of our security controls.

7. Security operations

U.S. Xpress maintains and regularly tests incident response and business continuity plans. Secure logging and monitoring are enabled across our information systems. We maintain a 24x7 Security Operation Center which enables the company to respond to threats.

8. Software development and security

U.S. Xpress uses security in the Software Development Lifecyle (SLDC). Security controls are enabled across our software development environments. Security controls are implemented and monitored with third party development as appropriate.