PACKER · THOMAS
Certified Public Accountants & Business Consultants

expedient

INDEPENDENT SERVICE AUDITORS' REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM

BASED ON CRITERIA SPECIFIED IN SERVICE ORGANIZATIONS CONTROLS NUMBER 3

SOC 3

SECURITY, AVAILIBILITY, AND CONFIDENTIALITY

For the period October 1, 2016 through September 30, 2017

Contents

PACKER · THOMAS
Certified Public Accountants & Business Consultants

6601 Westford Place,
Suite 101
Canfield, Ohio 44406
330-533-9777
1-800-943-4278
www.packerthomas.com

SECTION I - REPORT OF INDEPENDENT AUDITORS

CONTINENTAL BROADBAND

Approach

We have examined Management's assertion that Expedient maintained effective controls over the Data Center System ("the System") to provide reasonable assurance that:

- the System was protected against unauthorized access (both physical and logical),
- the System was available for operation and use, as committed or agreed, and
- information designated as "confidential" is protected as committed or agreed

during the period October 1, 2016 through September 30, 2017 based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Principles and Criteria)* throughout the period October 1, 2016, to September 30, 2017. We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the HITRUST Common Security Framework Version 8 Level 1 control specifications (HITRUST CSF requirements). Expedients' management is responsible for this assertion. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether Management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about Management's assertion, which includes (1) obtaining an understanding of Expedient Data Centers' relevant controls over the security, availability and confidentiality of the System and HITRUST CSF requirements; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Expedient's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, confidentiality, and HITRUST CSF requirements are achieved.

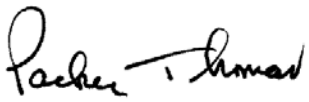
Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and

sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, Expedient's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, confidentiality, and HITRUST CSF requirements.

Packer Thomas



Canfield, OH
November 30, 2017

ASSERTIONS BY MANAGEMENT OF EXPEDIENT

We have prepared the description of Expedient's system for providing colocation and managed services to customers during the period October 1, 2016, to September 30, 2017. The description is intended to provide users with information about the data center system for colocation and managed services particularly system controls intended to meet the criteria for the *Security, Availability, and Confidentiality* principles set forth in AICPA, TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy and the applicable requirements set forth in the HITRUST CSF version 8 (HITRUST CSF requirements) as noted in the description.

We confirm, to the best of our knowledge and belief, that the description fairly presents the data center system throughout the period October 1, 2016, to September 30, 2017, based on the requirements set forth in the HITRUST CSF:

The description contains the following information:

1. The types of services provided and the applicable HITRUST CSF requirements
2. The components of the system used to provide the services, which are the following:

    a) **Infrastructure** - The physical and hardware components of a system (facilities, equipment, and networks).
    b) **Software** - The programs and operating software of a system (systems, applications, and utilities).
    c) **People** - The personnel involved in the operation and use of a system (developers, operators, users, and managers).
    d) **Procedures** - The automated and manual procedures involved in the operation of a system.
    e) **Data** - The information used and supported by a system (transaction streams, files, databases, and tables).

3. The boundaries or aspects of the system covered by the description
4. How the system captures and addresses significant events and conditions
5. The process used to prepare and deliver reports and other information to user entities and other parties
6. If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls
7. For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Expedient's system
8. Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria
9. Relevant details of changes to the service organization's system during the period covered by the description

The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

We further confirm that, to the best of our knowledge and belief, the controls stated in description were suitably designed and operated effectively throughout the specified period to meet the applicable trust services criteria.

Note: A signed original of this document is on file.

SECTION II—DESCRIPTION OF THE SYSTEM PROVIDED BY EXPEDIENT

Introduction to Expedient

Continental Broadband, doing business as (dba) Expedient provides managed hosting services to commercial clients. Expedient was acquired in 2005 by Continental Broadband Inc. (CBB). Prior to the acquisition, Expedient was a privately held entity that evolved and grew out of a series of mergers and acquisitions of commercial Internet Service Providers and fiber based, data transport companies throughout the east coast of the United States. CBB owns and operates data centers in several markets, including Baltimore (2), Boston, Cleveland (2), Columbus (2), Indianapolis, Memphis and Pittsburgh (2).

Expedient initially built a significant base of commercial clients utilizing Ethernet-based telecommunication services for Internet and private data transport. Since being acquired by CBB in 2005, the Company has successfully expanded its role in the provision of colocation, cloud and managed hosting services. Its data center facilities are the hub of its network in each geographic market. Within each data center, Expedient's experienced team of System Engineers provide management of customer computer systems, Storage Area Networks (SAN), Remote/Network and Remote Data Storage Solutions, Firewall Support, Load Balancing and a full suite of complementary Managed Hosting Services. The combination of its unique market position and mature connectivity business enables Expedient to bundle multiple products that create a link between the customer's user group locations (typically its working offices) and its critical business applications, which are hosted and managed at one of its data centers. This allows the target customer group, the commercial enterprise and professional service firms, to concentrate on their own core competencies without the need to employ a full suite of IT and IS resources to ensure that their critical technology applications are always available. This capability results in loyal, high-value customer relationships with low, to no customer turnover.

Expedient operations are headquartered in Pittsburgh, Pennsylvania where a staff of highly skilled network and system engineers provide oversight and support services to more than fifteen hundred core customers. The Cleveland, Boston, Baltimore, Columbus and Memphis offices staff according to operational demands, are responsible for providing local market sales, service and engineering support. All data center locations are staffed 24 hours a day, 365 days per year so that Expedient customers have the peace of mind knowing that they can always receive immediate, hands on support should the need arise. Operations Support Centers (OSC) in each of the data centers are integrated and virtual, with a sophisticated suite of "high availability" device monitoring tools, customer relationship management (CRM) software programs, IP telecommunications systems and physical security packages to ensure a consistently high standard response and resolution protocol. The markets are connected by a diverse and fully redundant, multi-gigabit, Ethernet transport ring, providing operational efficiencies and unique capabilities that most competitors cannot match. This structure creates a competitive differentiator for clients who are looking for multi-market hosting solutions, most often for the purpose of disaster recovery.

Operations

For a complete overview of the capabilities and technical features of each of the Expedient's locations, as well as an introduction to the data centers operated by its CBB sister companies, specifications and virtual tours are provided at:

https://www.expedient.com/the-data-centers/

OVERVIEW OF SERVICES

The company provides client solutions in these categories:

Backups – recover data following its loss or revert files to a state prior to a recent change by leveraging a best-in-class solution for peace of mind from hardware failure, software defects, human error and other common causes

Compliance & Security – satisfy a variety of industry and government mandates including Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley (SOX), EU-U.S. Privacy Shield Framework, Food and Drug Administration (FDA) Part 11 and more through the implementation of safeguards and the publication of third party attestations documenting process controls that are complementary to your own

Computing Infrastructure – reliably meet production or development availability and performance needs with tailored solutions that include the features your team needs to keep clients satisfied and grow your business

Disaster Recovery – continue critical technology infrastructure operations following the loss of function at a primary location through real-time replication and automatic failover responsiveness to maximize recovery time objectives

Storage – rely on the capacity and performance availability needed to safeguard critical data as your business grows

The company offers these services as part of its solutions:

Cloud – our hardware infrastructure expertise ensures the continuous performance and availability of your applications

- Public Cloud – maximum cost effectiveness
- Private Cloud – maximum segmentation for challenging compliance requirements and dedicated performance
- On-Site Private Cloud – an Expedient private cloud at any location
- Virtual Colocation – for teams already familiar with managing virtual computing assets
- Virtual Instance – for teams that want assistance managing virtual computing assets
- Disaster Recovery as a Service (DRaaS) – failover application environments with the push of a button between two or more of our data centers or your location and one of our data centers

Colocation – our data centers provide the perfect environment for your own physical assets as you establish your cloud presence over time

- Cabinets – lockable and dedicated to your equipment
- Cages – encompassing multiple cabinets and providing greater segmentation for challenging compliance requirements
- SlimLine Cages – encompassing multiple cabinets with maximum cost effectiveness to provide greater segmentation for challenging compliance requirements
- Power & Cooling – tailored to the unique needs of your hardware configuration to ensure peak performance and maximum life expectancy
- Remote Hands – our professionals are on-site 24x7x365 to provide assistance with physical requests so you can save travel time

Managed Services – our technology professionals deliver expert management and advice to enhance your team in the areas you need it

- Backup – consolidate heterogeneous systems and databases onto a standardized platform to enable recovery when you need it
- Data Encryption at Rest – protect unstructured data from unauthorized access using a key management server (KMS)
- Distributed Denial of Service (DDOS) Mitigation – real-time examination of network traffic to restrict suspicious flows and ensure a high quality of service
- Firewall – enforce access control to protect your critical data; choose optional failover capability to establish the most efficient recovery time objectives
- Intrusion Detection Service (IDS) – inspect network traffic to identify malicious packets for further analysis by clients
- Load Balancer – scale applications by distributing user session workloads across multiple servers
- Microsoft Active Directory – centralize authentication, group security policy, print services and other process standards
- Operating System – let our team manage security patching, anti-virus and other tasks that distract you from your strategic priorities
- Push Button DR – replicate workloads using software defined networking and dynamic routing protocols to move all workloads – and public IP addresses – seamlessly between different geographic locations
- Storage – choose from a variety of options that match your needs for performance and cost
- Two-Factor Authentication – protect your systems from unauthorized access with a one-time password
- Unified Log Management – record and archive system events for remediation and forensic purposes

- Virtual Private Network – protect your data in transit with encryption
- Vulnerability Scanning – validate information technology infrastructure through analysis of known vulnerabilities

Networking – our data centers are connected to each other, the world's largest networks and your locations to enable a converged infrastructure capable of serving your whole team

- Ethernet Anywhere – connect external locations in the same city to Expedient
- Wide Area Network – connect any external locations to Expedient, including through the use of software defined networking (SDN)
- Internet Access – connect to public networks
- Inter-Data Center – transport data between Expedient facilities

Learn more about Expedient services at http://www.expedient.com.

DESCRIPTION OF THE SYSTEM

Controls are generally described in five areas: Organization and Administration, Physical Security and Environmental, Electrical and Mechanical Systems, Change Management, and Disaster Recovery. While specific controls are not repeated here, in Section II, complete control objectives and control activities can be found in Section III of this report along with the auditor's findings, exceptions and commentary. Expedient implemented controls that map to HITRUST CSF v8.0 level 1. The following provides business justification for Expedient's decisions regarding the applicability of HITRUST Common Security Framework v8.0 Level 1. 54 of 66 critical controls are implemented as applicable. The following controls have been described as not applicable to Expedient for the represented justifications.

HITRUST Requirement Number	HITRUST Requirement	Justification
06.d	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and contractual clauses.	Expedient provides managed services and colocation services to a variety of clients, including those who process sensitive information through Expedient's infrastructure in use for health care, e-commerce and other related services. Expedient does not have any specific responsibilities or direct access to customer data.
09.e	It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party.	Expedient does not access sensitive information and does not use third party services for handling sensitive information.
09.m	Networks shall be managed and controlled in order to protect the organization from threats and to maintain security for the systems and applications using the network, including information in transit.	Expedient customers are responsible for ensuring that data is encrypted in-transit. Customers may or may not purchase relevant services to facilitate such encryption.
09.n	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	Expedient is a network service provider. Customers can purchase a variety of network configuration options at their discretion to create a topology that meets their own business requirements.
09.o	Formal procedures shall be documented and implemented for the management of removable media.	Expedient does not use removable media to perform colocation and managed services. Customer data does not reside on removable media.
09.s	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication mediums.	Since Expedient is an infrastructure provider, customers define policies, procedures and controls for exchanging information.
09.aa	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	While Expedient logs important information related to operating infrastructure, logging user activities related to accessing sensitive data is the responsibility of Expedient's customers. Customers may or may not purchase relevant services to facilitate such log auditing

HITRUST Requirement Number	HITRUST Requirement	Justification
		at their discretion.
10.b	Data input to applications and databases shall be validated to ensure that this data is correct and appropriate.	Expedient does not provide application or database entry services.
10.f	A policy on the use of cryptographic controls for protection of information shall be developed and implemented, and supported by formal procedures.	Expedient customers are responsible for cryptographic controls. Customers may or may not purchase relevant services to facilitate such cryptographic controls at their discretion.
10.g	Key management shall be in place to support the organizations use of cryptographic techniques.	Expedient customers are responsible for cryptographic controls.
10.h	There shall be procedures in place to control the installation of software on operational systems.	Expedient's customers are responsible for installation of software on their operational systems.
10.l	Outsourced software development shall be supervised and monitored by the organization.	Expedient does not outsource software development, nor does Expedient provide outsourced software development.

Organization and Administration

The governing structure promotes internal controls from the "top-down." Management communicates their aims to employees in a structured manner so that objectives are achieved.

Management has a clear division of responsibilities to help ensure that operations run smoothly and a system of internal controls and segregation of duties can be enforced. Segregation of duties is established through lines of reporting and enforced with logical and physical access controls. Specific areas of responsibility are clearly defined and access control is predicated on the employee position and job function. A formal organizational chart clearly identifies positions and responsibilities.

A core set of business values is established and documented to govern ethical behavior. A Code of Ethics formalizes the Company's business culture. The Code of Ethics covers topics including, but not limited to:

- Conflicts of interest
- Bribes and kickbacks
- Accurate and complete accounting and disclosure
- Anti-competitive conduct and fair pricing
- Confidentiality/Privacy of information of business partners and customers

The Code of Business Ethics also includes examples of items that should be disclosed and activities that are expressly prohibited. Expedient's Managers are responsible for familiarizing employees with this code. Managers are responsible for seeing that the employees and their supervisors are following this code in their business conduct and dealings. The Code of Ethics is incorporated into the Employee Handbook.

Policies and procedures and software solutions have been established to support Expedient's processing activities, customer support, and implementation of internal controls. Expedient has formal written policies, procedures and software to support business functions. Some additional detail on key processes is included at the end of this report for customer use. Policies, procedures, and software solutions include, but are not limited to:

- Policies and procedures for various functional areas
- Checklists to assist in implementing policy
- Detailed descriptions of key systems and controls related to the systems
- Ticketing system software (Support Management Console (SMC)) for customer requests and problems, change control, and task management
- Disaster recovery information
- Employee Handbook (contents include acceptable use guidelines)

Expedient has programs in place to help ensure that competent, ethical people are hired, and appropriately trained and evaluated. The Company facilitates third party criminal background and drug use screening as part of the hiring process. Pre-employment screening due diligence includes:

- Multiple Personal Interviews
- Work History Verification
- Personal Character References
- Street Drug Screen
- Criminal Background Conviction Screen
- Cognitive Ability and Job Skills Testing

Candidates applying for technical roles are required to demonstrate skills and competencies by responding to example questions and may be asked to complete assigned tasks in a lab environment simulating various conditions or circumstances. Further verification of education and certification achievement may also be pursued when necessary. Employees are trained on-site under the supervision of knowledgeable employees.

Expedient has a formal evaluation system. Expedient's performance objective and measurement tool, Partners in Performance, has three main components:

1. ***Performance Planning*:** The employee is asked to set personal performance objectives jointly with a team leader; the objectives are aligned with those of the employee's work team, department, the Company and Landmark (parent company).
2. ***Coaching and Feedback*:** The employee receives continuous feedback on performance from a variety of sources. These may include a team leader or supervisor, fellow team members and internal and external customers.
3. ***Performance Review*:** A formal review of an employee's performance is done at least once a year and should supplement ongoing feedback. During this process, the employee completes a self-assessment and discusses it with a team leader.

Project Management

To create a standard internal framework of products and services for operations personnel to implement, new customer requirements are translated by a project management process. A dedicated project manager is assigned to the implementation to be the single point of contact for the customer. The Company uses a traditional approach to project management:

- ***Initiation*** – Expedient conducts an internal contract/project review within a week after contract signing so that the sales/sales engineering team can convey the unique requirements of the individual customer in relation to the standard products and services chosen to meet them.
- ***Planning*** – The project manager will lead the process of establishing the chronology of events necessary to successfully complete the implementation. Consensus will be sought to finalize a definitive timeline to proceed to the execution phase.
- ***Execution*** – The project manager will aggregate regular updates from the various subject matter experts and conduct weekly update calls/meetings with the key customer contact to report on progress.
- ***Monitoring*** – The delivery and sales engineering teams meet weekly to review project milestones and react to inevitable exceptions.
- ***Completion*** – The project manager will verify that all services specified in the contract have been delivered and facilitate a transitional relationship with the Operations Support Center (OSC) for post-implementation support.
- ***Follow Up*** – The project manager or a member of the OSC management team will check back with the customer after several weeks of production implementation to review their experience.

Risk Assessment

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the Description of the System. Management has implemented a process for identifying relevant risks. This process includes

estimating the significance for identified risks, assessing the likelihood of their occurrence and deciding about actions to address them. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting the system.

Establishing Control Objectives

Expedient manages a variety of risks from external and internal sources, and a precondition to effective risk management is establishing basic controls and overall control objectives that align these internal and external conditions with our Company's tolerance of risk.

Risk Identification

Regardless of whether the objective is stated or implied, Expedient's risk-assessment process considers all risks that may occur - it is important that risk identification be comprehensive. Expedient considers significant interactions between itself and relevant external parties that could affect our ability to provide reliable services when establishing internal controls.

Expedient management considers both internal and external risks including:

External Risks

- Changing customer needs or expectations that could affect service offerings/development, operational processes and service, pricing or warranties.
- Technological developments that could affect the nature and timing of various service offerings.
- Competition that could alter marketing or service activities.
- New legislation and regulations that could force changes in operating policies and strategies.
- Acts of nature and catastrophes that could lead to changes in infrastructure, operations or information systems.
- Economic changes that could have an impact on decisions related to financial, capital expenditures and expansion.

Internal Risks

- A disruption in information systems processing that could adversely affect our ability to operate.
- The quality of personnel hired and methods of training and motivation that could influence the level of control consciousness within our organization.
- A change in management responsibilities that could affect the way certain controls are affected.
- The nature of Expedient's activities and employee accessibility to assets that could contribute to misappropriation of resources.

The risk management process focuses on supporting management's decisions and responding to potential threats by assessing risks and identifying important controlling factors. The risk management process provides assurance that Expedient's management decisions are implemented with predictable outcomes.

Risk Analysis

Expedient's methods for analyzing risks vary largely because our Company's risks are difficult to quantify. The process usually involves:

- Estimating the significance of the risk, including severity of impact on operations.
- Assessing the likelihood of the risk occurring.
- Considering how the risk should be managed.

Once the significance and likelihood of the risk is assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood that the risk occurs, including reviewing existing controls and establishing new controls.

Specific to the area of compliance risk, processes exist to monitor and assess current and new federal regulations. The Executive team of Expedient is on mailing lists and keyword search notices to stay in touch with any pending or recently passed regulations that may or may not affect the business. Expedient's parent company retains service of legal counsel, Wilcox & Savage, Norfolk, VA, to advise on any and all regulatory questions, requirements, filings and other compliance assistance. Expedient has adopted an Acceptable Use Policy, Expedient Terms and Conditions for Use of Service, which all users of Expedient services are bound. The Acceptable Use Policy requires lawful use of services and respect of rights of other parties. In addition, among other provisions, the policy covers web content and prohibited user activities.

Expedient Corporate Information Security

Expedient implements information security practices to protect the confidentiality and integrity of customer and company data systems. Expedient has instituted a Security Awareness Policy to communicate security expectations to the Expedient professionals through use of orientation for new employees and periodic Security Awareness bulletins for existing employees.

Before being granted access to Expedient facilities all visitors must sign in on the visitor log, which is reviewed and verified by authorized team members, and obtain visitor badges for identification purposes.

Controlled building access and secure access to specific areas are ensured through the administration of proximity cards and/or biometric devices at each location. Physical access restrictions for personnel are enforced with the use of an ID badge system, proximity access cards, and biometric access devices. Logical access to core networking equipment and customer resources is granted only to those personnel in roles that require such access by requiring passwords for access. To effectively manage security incidents, an Incident Response Process has been instituted, which outlines the procedures for responding to security incidents. This process is further defined below.

General Physical Security and Environmental Controls

Each data center is a single purpose facility engineered to address security and network redundancy, enabling Expedient to offer high availability to its customers. The below description of the data centers' environmental and physical access controls includes controls that are common to all data centers in scope; however, certain data centers have additional controls to supplement those described in this report.

Electrical and Mechanical System Controls

Data centers feature redundant HVAC (Heating Ventilation Air Conditioning) units which provide consistent temperature and humidity within the raised floor area. HVAC systems are inspected regularly and air filters are changed as needed.

Data centers are equipped with sensors to detect environmental hazards, including smoke detectors and water detectors. Data centers are equipped with fire detection and suppression systems and hand held fire extinguishers. Fire detection systems, sprinkler systems and chemical fire extinguishers are inspected at least annually.

Data center and office facilities are equipped with uninterruptible power supplies (UPS) to mitigate the risk of short term utility power failures and fluctuations. The UPS power system is redundant with instantaneous failover in the event of a primary UPS failure. The UPS systems are inspected on a monthly basis.

Data center and office facilities are equipped with diesel generators to mitigate the risk of long term utility power failures and fluctuations. Generators are tested monthly and maintained to provide assurance of appropriate operability in the event of an emergency. Expedient personnel are on duty 24/7 at all Expedient's data center facilities.

Data Center Physical Access

The data centers are highly restricted areas which require a much greater level of security and access control than traditional office spaces. As such, only individuals with express authorization may enter these areas. Access privileges will only be granted to individuals who have a legitimate business need to be in a data center area.
Facility access is unescorted in the case of employees and certain contractors who hold assigned electronic keys. Facility access is escorted for all other visitors including all customers who must check in and out, and wear a temporary identification badge.

The data center Access Control Log must be properly maintained at all times. The Log is maintained by Operations Support Center (OSC) staff and a self-service Visitor Access Management (VAM) kiosk system. All individuals with Controlling Access to the data center are responsible for maintaining the integrity of this log. The following procedures are followed:

- Each time an individual with Escorted Access to the data center is admitted to the area, he/she must properly "Check In" on the Access Control Log at the time of entrance. The person admitting the visitor must countersign and fill out the appropriate section of the form located within the Support Management Console (SMC).
- Each time an individual with Escorted Access leaves the area, he/she must properly log out on the Access Control Log at the time he leaves (even if only for a short time). The person with Controlling Access to the area who allows the visitor to leave must fill out the "Check Out" section of the Access Control Log.
- The VAM facilitates ingress and egress of all unescorted visitors including all customers, certain contractors and any other visitors who are not employees of the Company including but not limited to interviewees, business partners and family members.
- The primary components of the system are Visits, Scheduled Visits, and Visitors, as each visit is independent of Scheduled Visits and a scheduled visit could generate one or many visits.
    - *Visitors* – a list of every person who has visited a facility or has a scheduled Visit
    - *Visits* – a list of all check in, verify and check out activity
    - *Scheduled Visits*
- Authorized – Visitors on distinct customer escalation lists in the SMC are authorized for entry into our facilities; Users with administrative privileges in the SMC have authorization to grant access to other Users or anyone else.
- Ad Hoc – Visitors for which there is no SMC relationship and must be added to a scheduled visit via direct input. A Visitor who registers at the kiosk will appear on the 'Arrived' tab and in the 'All visitors' tab. Any person identified by a User with Visit Administrative privileges may be granted access.

All escorted visitors are required to present a valid photo identification card to verify their identity whether or not their visit is scheduled.

Shipping, Receiving & Limited Short Term Storage

This policy and its accompanying procedures are used to ensure that all shipping, receiving and limited short term storage requests from customers are processed and tracked in a consistent manner.

Scheduling Shipments

Inbound and outbound shipments may be scheduled by Customers through the Support Management Console (SMC) at https://support.expedient.com or by calling the Expedient Operations Support Center (OSC).

All outbound shipping from Expedient facilities must be scheduled 24 hours in advance through the Support Management Console (SMC) or by phone through the Operations Support Center (OSC). Customer must communicate all specifics in writing and prepare parcels for shipment. Expedient does not provide packing material.

All inbound receiving of shipments to an Expedient data center must be scheduled 24 hours in advance through the Expedient Support Management Console (SMC) or by phone through the Operations Support Center (OSC). Only scheduled shipments will be accepted for delivery.

Expedient shipping areas were designed for just-in-time shipping arrangements, meaning there is limited space for storage. Limited short term storage can only be provided for a maximum of 3 business days.

Limited Short Term Storage of Received Customer Shipments at Expedient

Expedient will store a Customer's received deliveries for up to three business days after they've been notified of the delivery. If the delivery hasn't been retrieved after that time, Expedient will contact the Customer and attempt to make arrangements for retrieval. If no acceptable arrangements can be made, Expedient may have to return the delivery to the address of origination at the Customer's expense or begin charging storage fees at its discretion for each day beyond three. Expedient regrets that it cannot provide long term storage due to space constraints and security policies.

Removing Equipment from Expedient

Expedient requires that removal of equipment that was not brought in the same day must have a valid service request submitted at least one (1) business day (Monday – Friday) in advance and be notated with the quantity and description of the items to be removed. All items whether loaded to a truck from the dock or hand carried from the lobby must be verified with OSC personnel including, but not limited to documentation of quantity, make, type, model, serial number and any other identifiable information.

Digital video cameras monitor the data centers and points of ingress/egress. Digital video recordings are maintained for a minimum of 90 days.

Wireless Network Access

The Company maintains two separate wireless access zones for use by employees and visitors:

Employee Wireless Access Zone (wireless.expedient.com) – is facilitated by the corporate Microsoft Active Directory and requires valid credentials. PCs connected to the corporate Windows domain are automatically authenticated upon login while handheld devices (Smartphones, etc.) require a username and password to be entered manually. Employees have access to internal vLANs when connected to these access points similar to the wired network.

Visitor Wireless Access Zone (customer-wireless.expedient.com) – is open to anyone. Acceptance of the Company's terms and conditions of use of service (TCUS) is required by clicking a button in a web browser before access is granted. Access is limited to the public Internet and is provided as a professional courtesy to customers, vendors and other visitors. It is not possible to access internal vLANs from these access points.

Wireless access is monitored closely by the Company. The Operations Support Center audits wireless access points on a monthly basis using NetStumbler to scan for vulnerabilities and to assess the needed base level of security relevant to the affected network.

Network Security

Colocated customer servers and devices are located on separate VLANs, a switched network that is logically (not physically) segmented on common networking equipment. In VLAN technology, packets are switched between ports designated within the same VLAN; all broadcast traffic is contained within a particular VLAN. Every colocated customer has a separate VLAN. Typical customer implementations include a "public", or Internet-facing VLAN, and at least one "private" VLAN.

Across the Expedient network, the BGP exterior gateway protocol is utilized to exchange routing updates between peers, upstream transit providers, and the subset of Expedient customers who employ BGP within their own networks.

Customer-facing BGP sessions are subject to MD5 neighbor authentication at the customer's discretion. Additionally, access control lists are applied to these sessions on ingress, which include only those IP prefixes under a given customer's control. The customer's right to announce these prefixes is verified by ARIN records at the time of the customer's service activation. (The American Registry for Internet Numbers (ARIN) is a non-profit agency who handles registration and dispensation of Internet protocol addresses in North and South America.) Any announcement or routing update which falls outside the scope of these access lists is ignored by the Expedient network.

SERVICE DELIVERY

Operations Communication System High Availability

Communication is a critical component of the services that we provide. In order to ensure the reliability and availability of the systems required to keep in touch with key stakeholders, the Company made a significant investment to implement fault tolerance. By applying proven redundant routing and call/message flow techniques with carrier-class equipment and software, unified voice-over-IP and email communication system architectures were chosen.

The Company publishes both national toll-free customer service telephone numbers as well as local direct inward dialing (DID) numbers. The core system facilitates menu options, routed skill-based queues, pre-recorded messages, voicemail and many other functions that are relied upon to function normally, especially in emergency situations.

The core call processing hardware and circuitry functions of the system are mirrored between two of the Company's data center locations taking advantage of the inherent redundancies built into the physical plant.

Exchange 2013 is utilized to provide e-mail services for Expedient staff. E-mail is a critical function to our business. It is used to communicate internally to employees and externally to our clients. Additionally, it is integrated into the voicemail system and is the backend storage for voicemails in the enterprise.

The systems are tested from time to time when unplanned events occur that affect network connectivity. Planned disaster recovery testing is scheduled to occur once a year when more extensive failures can be simulated and validated at a time when business operations are least impacted.

Support Management Console

The Operations Support Center (OSC) is the focal point for management and monitoring of the Expedient network 24x7x365. With the assistance of cutting edge visualization software the OSC proactively ensures reliability of the network and reacts to unplanned events. It is primarily responsible for problem resolution and coordinates troubleshooting internally and with third parties. Customers utilize the Support Management Console (SMC) as a dashboard to take advantage of self-service so they can:

- gain visibility to service related requests, create new ones, track updates (or add their own) and review history;
- manage authorized users' contact information, permissions, facility access, notification preferences and more;
- view authorized visits including check in and check out dates and times;
- stay up-to-date with archived notifications that provide details about planned maintenance, unplanned event root cause analysis and other service related information;
- view managed device assets view alert history including follow up actions;
- leverage resources to share files, view usage patterns, edit service attributes like DNS and obtain escalation information and;
- view account information and subscription services.

High Availability Infrastructure

Expedient utilizes fully redundant enterprise-class Juniper routing and switching equipment for its core networking infrastructure. Shared infrastructure routers and switches feature redundant power and connectivity to the Internet is provided by redundant fiber and Internet backbone connectivity providers. Expedient utilizes advanced route optimization technology to provide efficient routing among the various backbone carriers.

Expedient provides customers with a stable infrastructure including servers with Anti-Virus tools to protect its network. Expedient has created a comprehensive virus management solution that works to prevent virus infections and automates the virus definition updating process. Tools are used to scan servers for viruses and infected files are automatically quarantined unless otherwise requested. Expedient maintains current virus signature updates to ensure networks are protected from newly developed threats. Expedient uses several tools that proactively detect and trace network-wide anomalies, including distributed denial of service (DDOS) attacks and worms. Through network-wide, router-based sampling, Expedient evaluates existing and potential threats by aggregating traffic from across the network using the Arbor Networks Peak Flow SP (service provider) appliances for detection and prevention. Expedient uses remotely triggering black hole (RTB) filtering technology on its border routers to automatically reject suspicious traffic as quickly as possible.

Multiple transit relationships guarantee that (1) a single failure in transit service will not make a site hosted from Expedient inaccessible, and (2) virtually all Internet customers can reach sites hosted on servers residing at Expedient's data center.

Connectivity is achieved through redundant dark fiber paths. Expedient owns the electronics which lights the fiber. Expedient connects to a diverse range of Tier 1 Internet providers. The contractual arrangements assure that all visitors can reach sites hosted at Expedient. In addition, IBM NETCOOL is used to monitor Internet connectivity.

Configurations of network infrastructure IP devices are regularly backed-up so a restore can be made to a current configuration at any time. Configuration snapshots are automatically archived nightly to the TACACS+ Server via SNMP-triggered TFTP uploads.

Multiple DNS servers provide for redundancy in resolution services. Expedient has five authoritative name servers and ten (10) resolving name servers located in different physical locations. Physical locations maintain at least one authoritative server and two resolving servers. Authoritative servers house primary (hosted) DNS data, and provide redundancy in that the data is replicated between the servers which are situated in geographically diverse locations. Resolving servers host cached data, and they are used as DNS servers for all lookup requests from clients in a particular physical location; to provide redundancy, two resolving servers are located in every physical location. The location of the DNS servers creates fault tolerance in name resolution services.

Replacement parts and spare IP devices are available for quick replacements of faulty components. Expedient maintains an inventory of replacement parts and backup networking equipment to ensure rapid recovery in the event of hardware failure.

Capacity is monitored to meet operational and customer needs and to plan for growth. Internally, Expedient utilizes CACTI Application Performance Management software to monitor all links for capacity issues and line errors. CACTI provides network performance information to help pre-empt problems and optimize resources. Active SNMP polling of statistics relating to system resources (such as core switches, distribution layer switches, shared firewall cluster, and monitoring station) and link utilization is performed by the CACTI monitoring server.

CACTI is also made available to customers to monitor their individual resources, such as circuits, CPU and memory for capacity matters. Active SNMP polling of statistics relating to system resources and link utilization is performed by the CACTI monitoring server for customers who request the information.

INFRASTRUCTURE MAINTENANCE AND CHANGE MANAGEMENT

Overview of Shared Infrastructure

Expedient shared infrastructure represents any component of the communications network or physical environment that is not customer specific. Shared infrastructure is utilized by more than one Expedient customer to gain economies of scale for appropriate types of equipment.

Change Control Controls

The following change management policy applies to all changes -- including changes to infrastructure and managed services.

Expedient has a formal policy that outlines procedures for change management; the procedures must be acknowledged with the employee's signature. Expedient requires absolute adherence to the policy; failure to use the process as described in the change management document or failure to involve others in the face of uncertainty results in disciplinary action.

Changes are approved prior to being put into production. For all changes governed by the Change Management Policy, the Engineer must complete a CMS Form that includes a project plan, a rollback plan and a monitoring plan. Approvals for each part of the change plan must be obtained.

Project Plan - The project plan includes the steps that must be completed to make the change in a checklist format. The Project plan must have at least one peer approval.

Rollback and Monitoring Plan - The rollback plan includes the list of steps that will be used if the change proves ineffective and must be reversed in a checklist form. The rollback plan must have at least one peer approval.

Regularly scheduled formal change control meetings are held to review change controls plans and to facilitate communication. Representatives from key operational areas attend the meetings. In these meetings, the change plans are reviewed, arrangements are made for customer service representatives to notify customers about planned outages, and previous changes are reviewed. At each change meeting, the change controller, an OSC representative for the change period, and the Single Point of Contact (SPOC) for each engineering organization are required to be present.

Changes are implemented during established timeframes to minimize disruption and facilitate communications. Standardized change periods are designated during each week so that change and communication of upcoming changes occurs in a structured manner. The change period is the interval between the time when a change is proposed and the time that it is scheduled to be implemented. This timeframe is established to allow the OSC adequate time to notify affected customers of upgrades. The change period generally starts at least 72 hours after the change meeting. This leaves enough time for customers to be contacted about upgrades and the possible loss of service.

That status of changes is tracked, monitored, and communicated throughout the organization. A change control log is maintained to track the status of all changes.

- *Date & Time* – date and time when change is scheduled to occur
- *Purpose & Details* – a brief description of why the change is to be performed as well as a quick overview of the change itself
- *Performed by* – the engineer responsible for the change
- *Rollback* – a brief description of what steps will be taken in the event of a rollback
- *Monitoring* – a brief description of steps taken to confirm the change completed as planned
- *Internal notification* – The internal notification is a yes/no answer. Depending on the change, an internal notification to employees may or may not be sent out.
- *Customer notification* – This field will either be the name of the customer service person who is going to notify the customers of the change or an "n/a" if they decide not to notify customers of the change. The choice to notify (or not) is made by the appropriate customer service representative.
- *Status and comments* – any relevant information to the change. This may be a status, more detail on the change, a reschedule date, or other necessary information.

Patching Deployment

Patch management procedures define lines of communication. All devices are subject to patch management deployment practices. Specific procedures are established for internal and external communication about patch installations, including who to send emails to, required email content, etc. Expedient has detailed written procedures that define the patch management process on a day by day basis. Expedient management has established methods to stay informed of security issues, potential vulnerabilities and patches. All Microsoft OS-based systems are tracked in a proprietary database with OS, Service Pack, Domain, Physical Location, and special instructions for patching. All Non-Microsoft OS-based systems are tracked in a proprietary database with OS, version and name. Microsoft patches are tested on non-critical and development servers before they are applied to production systems.

Managed Hosting Services

Controls described in this section "Shared Managed Hosting Services" relate specifically to all facilities when purchased from Expedient and includes the following shared service offerings. Not all Expedient customers elect these services. Changes to Managed Hosting environments are made using the above change management process. Services include:

- Managed Operating System Hosting
- Virtualization Services
- Data Protection Services
- Firewall Services

Managed Operating System Hosting

Logical access to resources by Expedient employees is granted or modified based on current job responsibilities. Only authorized Expedient employees have logical access to managed, dedicated servers. All users are assigned a unique ID and password.

For Windows, Active Directory (AD) group policy is used to define security on files and folders, set account policies and restrict access to resources through membership in groups. Users are granted rights to perform tasks and permissions to access resources by assignment to groups. Through group assignment, electronic segregation of duties is maintained. Access to resources is managed by Expedient Systems Engineering Group and Operations Support Center. Access control features within the platforms used to limit access to resources include:

- Groups
- Directories
- File ownership rights
- Group policy (Windows systems only)
- Computers

Directory Service features are used to segregate customer servers from Expedient servers. Expedient uses Windows domains as security boundaries. Customer servers and Expedient internal servers are segregated into two different domains.

Encrypted channels are used for all systems administration. In LINUX and other UNIX based hosts, secure shell (SSH) is utilized, and in Windows encrypted RDP is utilized.

Customer/Expedient servers are secured by selecting services, eliminating unnecessary protocols, and following best practices about role-specific security requirements.

In LINUX and other UNIX based servers - Expedient Engineers have a defined methodology for installing new LINUX and UNIX based servers; two checklists, a general checklist and a security checklist, are used to guide the process. In order to harden the server, settings are modified to increase security and tools are used to assess security prior to deployment. Procedures include, but are not necessarily limited to, the following:

- Disabling root logins
- Turning off most services
- Turning off all extraneous daemons
- Using IP tables to block traffic or create a firewall
- Restricting SSH to specific IP addresses
- Turning on system monitoring

Windows - By default, Windows servers are deployed with the following native security controls which are left at default values, except where a customer may dictate otherwise. Some of the native controls include, but are not limited to:

- FTP service is not installed by default
- Telnet is turned off by default
- By default, security events are logged to the Windows security event log
- Monitoring is turned ON

Anti-virus software is implemented and updated to help protect customer's programs, data, and other information resources from viruses. Expedient deploys Symantec End Point Protection with appropriate version control on all managed servers. Virus definitions are updated daily, and an automatic alarm is generated if the hosts do not receive updates.

Controls are in place to monitor use of account creation rights, to investigate suspicious activity and to maintain proper system availability through specific monitoring.

LINUX and UNIX Based Servers - Daily, alarms are created by entries to the messages log file. Based on the severity of the alarm, it is sent to the NETCOOL monitoring platform which is maintained by the OSC and reviewed upon generation.

Windows - Within the Windows Server environment, logs in the Event Viewer are reviewed for critical errors by the Systems Engineers.

Performance is monitored at the host level for high-availability systems. Expedient utilizes Microsoft's System Center Operations Manager (SCOM) for host monitoring for Windows. SCOM is used for both internal Windows servers and customers purchasing premium monitoring or OS Management in a Microsoft environment. Expedient utilizes SecretAgentMon (SAM) for internal UNIX/LINUX servers and customers purchasing premium monitoring or OS Management in a UNIX/LINUX environment. SCOM and SAM have interfaces into the NETCOOL system which is monitored by the OSC 24/7.

Cloud (Virtualization) Services

Expedient provides subscribing customers with a redundant virtualization cluster to ensure complete availability. Expedient utilizes VMware's VSphere Enterprise edition software, combined with servers to deliver highly reliable virtualization services. All Virtualization points of delivery (PODs) are composed of redundant hardware, consisting of redundant disk drives, power supplies, etc. The PODs themselves are redundant, meaning that if a physical server were to fail, there is additional capacity to allow for the virtual environments to all continue to operate with minimal affect to availability. The PODs utilize redundant network switches to ensure network availability and redundant storage.

Customers have logically segmented access to only their environments. If subscribed, customers may access the virtual machine administration system, known as VMWare vCenter. Customers are provided with unique IDs to identify them, and are only granted access to their individual server(s).

Data Protection Services

Expedient has implemented a strategy for cyclical backup of data and programs. Expedient utilizes various backup technologies software for distributed backup and recovery operations. For customers subscribing to the backup service, unless otherwise directed by the customer, daily backups are made of all content on the systems. If the customer is subscribing to tape based backup, the media is LTO based removable tape; if the customer is subscribing to disk based backup, the data is housed on a redundant array of independent nodes within a storage area network (SAN).

For those customers subscribing to off-site backup services, they may have their data (in part or in total) transferred over Expedient's private network storage systems in other Expedient markets.

Encryption is provided for customers specifically requesting encryption.

Backup jobs are reviewed for successful completion. The OSC is responsible for reviewing reports that indicate successful completion of backup jobs. Expedient uses IBM's NETCOOL application to collect and consolidate alarms and events. If a backup (optionally, data duplication) job fails an alarm is generated in the NETCOOL application. Expedient has written procedures for backup job failures and established escalation procedures. If a backup job fails, the OSC is alerted and will follow procedures as listed on Expedient's documentation site. Should the OSC be unable to resolve the issue, a case is sent to the Systems Engineering Group for further review and resolution.

All customers have the ability to receive backup alerts and reporting information. Customers may receive errors or both errors and success messages specific for their hosts via email. Additionally, customers receive weekly summary reports which detail the hosts being backed up and the data backup amounts.

Procedures are followed to periodically test the quality and effectiveness of backup/restore processes and the quality of backup media. In addition to the opportunity to review backup logs, customers are given the opportunity to test recovery. Instructions for using the back-up software Modules to restore files are available at customer request. Help is also available from OSC Analysts in performing restores.

Backup files stored on-site are in a secure location. Expedient deploys backup servers that are configured on the network with an attached tape silo for performing backups. Gigabit Ethernet switches make the connections. Backup tapes are locked in the tape silo. Physical controls include video monitoring and key-fob/card access to the floor. Expedient uses dedicated equipment for tape libraries. The tape library is locked, with the keys held in the Operations Support Center lockbox and in a locked drawer of the Primary Backup Engineer.

For data transferred electronically, the use of Expedient's private 10 Gigabit Ethernet WAN is utilized. Logical access controls to backups is provided. Managed Backup Services include the installation of the particular client on the

customer's server(s) by either the customer or Expedient personnel. Administrative access to the server is required to install such a client. Where this is not possible, the client is provided to the customer for self-installation.

After client installation, configuration is done on the backup server. The server, based on IP, is put into a particular group. Groups are unique to a particular customer. No two customers may be in the same group, but customers may have multiple groups. Within the application, ACLs limit a customer's access to files and directories. Only the server which backed up the data may restore it. This control is based on the server's IP. This ACL restriction may be relaxed should a customer desire that a server restore data from another of their servers. Access is granted by written request.

Firewall Services

Redundancy is used to provide continuous service. Expedient utilizes the High Availability Feature set for seamless fail-over for critical services. The firewall cluster eliminates the firewall being a single point of failure in a network. The firewall is monitored for performance and effectiveness; management is alerted to problem conditions. SNMP traps and SYSLOG messages are sent from the firewalls to the NETCOOL monitoring server for archiving, processing, and display to the OSC.

Monitoring practices are described in the following paragraphs:

- The firewall's performance is monitored by the NETCOOL system sending traffic through to the hosts behind it. A firewall issue affecting throughput would be reflected by this and cause an alert to be created in NETCOOL. NETCOOL alerts are escalated to the appropriate engineering as needed. Active SNMP polling of statistics relating to system resources and link utilization is performed by the CACTI monitoring server.
- Rule Sets are established and changed in a structured manner to ensure accuracy. The rule database can be viewed but not modified by OSC personnel; changes to the configuration of these devices are restricted to engineering and related support staff. Changes follow the standard Change Control process described in the Change Management section of the report, using a change request procedure and requiring a corresponding Ticketing case.

Within the change request process, Expedient has a structured methodology for making changes to firewall policies that helps ensure that the correct policy is applied for the correct customer. This structured methodology includes:

- Saving old copies of the policy before any changes are made
- Using a standardized policy naming convention that includes the customer name and device. Expedient maintains an historical record of all rule changes. Configuration backups are made of the entire rule/object database any time a change is made to the rule database.

Monitoring Internal Controls

Expedient performs monitoring activities in order to continuously assess the quality of internal controls over time. Monitoring activities are used to initiate corrective action through management meetings, conference calls, and informal notifications. Management performs monitoring activities on a continuous basis and necessary corrective actions are taken as required to correct deviations from company policy and procedures.

Examples of Expedient's ongoing monitoring activities are:

- In carrying out its regular management activities, operating management obtains evidence that the system of internal control continues to function
- Communications from external parties and customers corroborate internally generated information and indicate possible problems.
- Organizational processes, structure and supervisory activities provide oversight of control functions.
- External auditors provide recommendations for how internal controls can be strengthened.
- Training, formal and informal meetings with employees.
- Specific monitoring controls are in place and part of the services offered by Expedient.

CLIENT/USER CONTROL CONSIDERATIONS

Each customer using Expedient services must consider their own control environment and use due diligence in assessing the level of risk that may be acceptable for any asset that is colocated with the data center. The following paragraphs outline some internal control responsibilities that must be evaluated by a customer in developing each customer's unique risk assessment. In addition to these items, other internal controls may be necessary which are not considered here.

1. Customers are responsible for reporting any problems to Expedient as soon as encountered. Customers are also responsible for assisting Expedient in responding to the problems.
2. Customers are responsible for carefully assessing and understanding their backup requirements and choosing backup plans in accordance with their internal risk assessments. Customers must work with Expedient representatives to ensure that they have chosen the right backup plan to balance the costs and the benefits of various backup strategies. There are risks that customers should consider, including but not limited to, the following:
    - Without choosing full archival (backup data kept forever) at periodic intervals, there is a possibility that there could be propagation of corrupted data.
    - When subscribing to "hot backup" database backup, transactions made between nightly full system backups may be lost (unrecoverable) if a database becomes corrupted.
3. Customers are responsible for testing restoration of files. Information regarding how to test restoration is available on-line or through the OSC.
4. Customers are responsible for reviewing backup logs which are made available upon request.
5. Customers are responsible for informing Expedient regarding any changes in the file system, operating system, or hardware platform that would require changes in backup processes.
6. Customers are responsible for assessing their need for daily duplicate data sets to be stored in two separate physical locations on a daily basis. Customers are also responsible for analyzing their need for off-site backup and encryption.
7. Customers should use effective (not easily guessed) passwords for all Expedient systems and customer-owned servers to which remote access is gained, and change passwords regularly. Customer is responsible for formulating an effective password policy.
8. Customers are responsible for promptly reporting any job position changes or terminations of employees who have remote access to data or programs maintained by Expedient as well as access to Expedient facilities.
9. Customers should never email confidential information, including passwords, to anyone saying that they are from Expedient without encryption and without verifying that the Expedient employee is authentic. Customers are responsible for educating themselves about social engineering attacks.
10. Customer is responsible for security controls over their own applications, data used by their applications, and the operating systems. In addition, if data is highly sensitive, customer is responsible for determining the need for, and providing, data encryption, system hardening, and scanning for vulnerabilities.
11. Customer is responsible for identifying upgrades that must be made to their systems.
12. If data or programs are highly confidential or disclosure or loss would result in extreme hardship, customer is encouraged not to use shared application platforms.
13. Customers must evaluate the need for redundancy within their systems and network architecture. Expedient provides multiple layers of redundancy, however, customers must subscribe to additional services to take full benefit of all applicable amenities.
14. Customer takes full responsibility for any contractor granted access to their systems or networking equipment by them. This includes physical access to the equipment provided by Expedient as indicated by written communication by the customer on record.
15. Expedient holds no liability for damages to any system or network element in the event any customer requests the use of "Remote Hands" to perform services that are not contracted for.