Data Security Compliance and Network Availability Overview

USAFact depends heavily on the use of computers in the day-to-day business activities of the company. The very core of USAFact's business is the sophisticated network that provides communication to not only our internal employees but also with our clients and global information providers. Vital functions of the company depend on the availability of our network of computers as both staff and clients rely upon our systems to perform their jobs and obtain our services, all of which are important to the well being of the company.

Equally important to the availability of our network is the privacy of the information we procure for our clients. USAFact has a long history of protecting consumer privacy continually increasing and improving upon our security efforts to protect the background and drug testing results.

This Security Overview outlines the measures utilized by USAFact to ensure compliance, security, and availability.

napbs
National Association of Professional Background Screeners
MEMBER

USAFACT™

Executive Summary

Attention USAFact Clients:

USAFact is proud to be the background provider for some of the most successful companies in the country. Our goal is to create partnerships with our clients and in keeping with that goal, it is important for us to educate our clients on our process and the controls over our process. The purpose of this review is to outline the processes and procedures USAFact utilizes in ensuring availability, security, and compliance as a data provider.

Network Availability

From backup power, to backup data, to an alternate facility, USAFact does everything necessary to ensure that our systems are available to our clients. The company has operated at a 99.999% uptime since the inception of our online system in 1998.

Data Security

The security of our data is of the utmost importance to the company and we take every precaution to ensure that our data only reaches its intended user. USAFact's online order and retrieval system is protected by industry standard security practices and software. All communications with USAFact systems are encrypted with industry-standard 128-bit SSL verified by Verisign.

Industry Compliance

The new century has been marred with scandal from careless information providers to accounting controversy in some of our nation's largest companies. As with any scandal, legislators took measures to guard against repeat offenders. USAFact complies with the systems security requirements for Sarbanes-Oxley, SAS70, HIPPA, and Graham Leach Bliley. Our systems are evaluated by Security Metrics to ensure exposure is never a problem. In addition to vulnerability studies, Security Metrics is also contracted to process penetration testing to ensure our systems are not susceptible to attacks or security breaches.

If you have any questions regarding any of the information on this review, please contact our IT Department at 800.547.0263.

Best Regards,
USAFact, Inc.

Table of Contents

USAFact Systems Security Table of Contents

USAFact is an Internet-based candidate screening company. Our Background Screening Information is secured by experienced professionals and a global network of skilled researchers who retrieve and report public records and data. Our clients rely on our services as important decision-making tools in creating safe and productive work environments. USA-FACT delivers information using state-of-the-art Internet technologies unique to the screening industry. Our objective is to create a partnership with our clients to develop the most efficient methods of delivering information to service their individual needs.

Partners

TransUnion
Quest Diagnostics
LabCorp
Driver Alliant Insurance Services
ERC DataPlus
Immigration Tracker

Affiliations

Nat'l Assoc. of Prof. Background Screeners
Society of Human Resources Managers [SHRM]
TransUnion Client Advisory Board
Drug and Alcohol Testing Association [DATIA]

napbs
National Association of Professional Background Screeners

TransUnion.

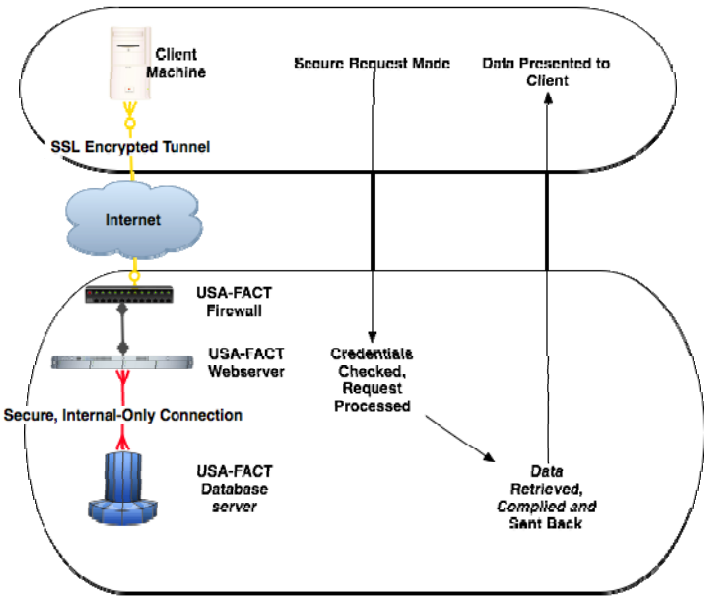
Member of the TU Client Advisory Board

Clientele

USAFact is a leading provider of pre-employment screening through effective utilization of three key elements to deliver an end product that is a "best fit" program for the specific needs and expectations of our clients, Customer Service, Technology, and Quality Assurance. USAFact has been very effective in screening candidates for a wide array of industries:

Financial
Medical/Healthcare
Distribution Centers
Government Municipalities
Construction
Equipment Rentals
Staffing Agencies
Food Service/Restaurant
Insurance
Security
Transportation
and More!

Our Network



Firewall Protected

The USAFact Firewall limits vectors of attack to the heavily monitored and guarded front entrance to the system.

Encryption

USAFact utilizes secure 128-bit secure socket layer encryption verified by Verisign and enforces external access over an encrypted channel to those accessing our online system.

Systems Security

USAFact operates a sophisticated infrastructure that enables our clients to safely procure background reports on the candidates they are considering for hire. Our client's connections are end-to-end secure, confidentially and securely communicating across today's complex, global networks. Every day, thousands of clients are able to safely access our system to retrieve the information they need to make intelligent hiring decisions, without needing a team of security experts. All communications with USAFact systems are encrypted with industry-standard encryption verified by Verisign.

USAFact deploys an intelligent system infrastructure necessary for everything from procuring background results to obtaining confidential drug screening results. Our protocols revolve around proactive security services to maximize prevention and increase the level of detection in our systems.

USAFact systems operate under the scrutiny of the providers we obtain information from. We are audited by several entities to ensure their own compliance making our security efforts twice as important to maintain.

Security Protocols

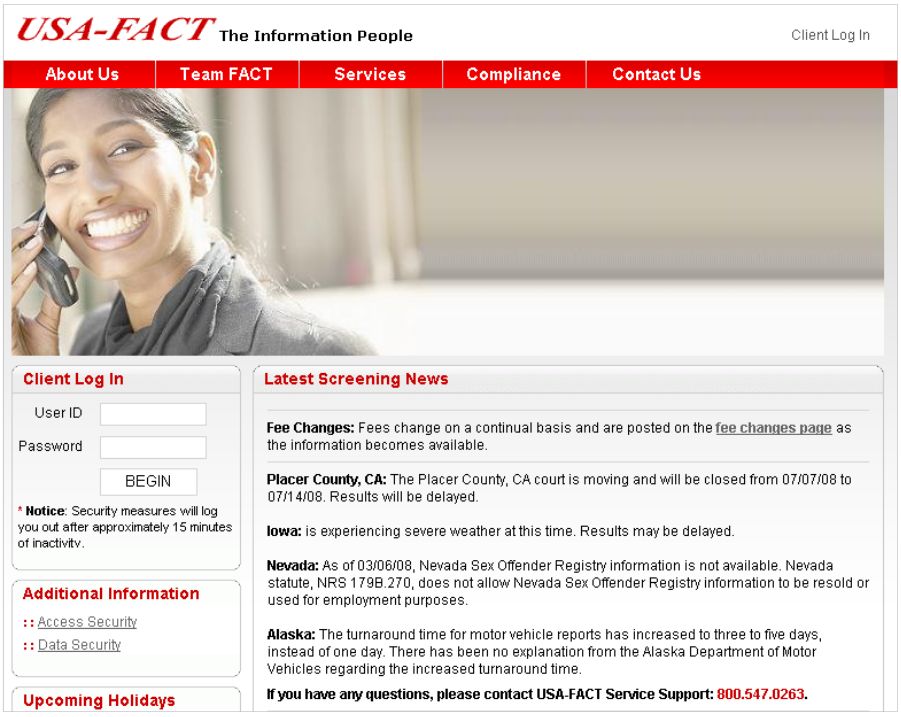
USAFact operates a segmented network. Our servers are responsible for one job each, and separated from each other. For example, if security is breached for one web server, security for the other servers remain intact therefore access to the mail server does not give you access to the database server.

Our intrusion detection protocols monitor all access for unusual patterns in addition to files on the system for unauthorized changes. Logs are printed and additionally sent to a secure server so they cannot be deleted after a compromise. We will always be able to track attacks.

USAFact monitors all sessions, allowing us to intelligently restrict access. This means that user-access times out or stops operating after inactivity. For example, if the user leaves their station, other employees cannot use that user's connection to pull up data. Individual user access is also revoked after a specified period of disuse.

Access Overview

Access into USAFact systems is limited to clients, vendors, and employees performing their jobs. We understand the nature of the business and go to great lengths to enforce Security Protocol.



Controlling Access

USAFact takes every precaution possible in providing access to the information procured each day for our clients. Access is controlled and monitored by several security features in our effort to provide our clients with confidence in our defense against identity theft.

Client Access

Clients new to USAFact must go through an extensive step by step identification process before we provide them access to our online system. Our agreement includes a business application for banking information and credit references and our protocol list includes a request for an onsite inspection, request for business license, an Internet search for articles pertaining to the company, phone listing search to ensure they are listed in the phone book, letters of incorporation, and the identity of the business owners.

Client activity is monitored daily and audited by security programs that flag suspicious activity. Client access is additionally controlled by the security parameters of the system.

Employee Access

Employee agreements are in place with each employee explaining the nature and importance of the job we perform. Peripheral storage devices have been removed from each employee's computer, access to outside email is denied to everyone in the organization, and email transmissions by employees are monitored for suspicious activity.

Employee access is regulated by regular password changes and the company's ability to immediately revoke access to the system. Access to employees is also limited to job function which restricts their access to only information required to perform their duties.

Vendor Access

Results from most outside vendors are first entered into quarantined database storage, where they are examined before insertion in the live USAFact database. Exceptions include credit and DMV information. Every precaution is taken to ensure that all data is accurate and safe before being admitted into our internal security ring.

Data Protection Policies

Procedures are in place to verify the identity of all people calling in requesting information. People are called back at the number on file for the account, identities are verified with the responsible person on file for the account, and pass codes can be implemented to prevent unauthorized changes. Security Level 5 client access contains the ability to view all active accounts for the entire organization with full audit ability to add and remove users.

Security Levels

User Account Monitoring

User accounts are password protected and monitored for misuse. Abuse of account privileges, such as running a report on one's self, are logged and can be traced back to the user that initiated them. Multiple Security Levels restrict access to authorized personnel. Accounts can be audited, created, modified or deleted by the primary account holder. All accounts are monitored for suspicious activity or lack of activity which results in account suspension. Accounts can be reinstated with a call to our Client Support Center.

Security Levels

USAFact understands the importance of securing information and providing appropriate access. We designed our USA-ONLINE software with six security levels to ensure that only appropriate personnel are accessing highly confidential information. These six security levels control access:

Access Level 0: Can only access a specific report or electronic invoice but cannot order or retrieve any reports.

Access Level 1: Input Only. This level was designed to allow data entry to be completed by clerical staff without providing them access to confidential background information.

Access Level 2: Input and Retrieval of only requests input by this user. This level was designed to allow staff managers to retrieve the confidential background information they have requested for their particular department.

Access Level 3: Input and Retrieval of only requests input within a location or user group. This level was designed to allow staff managers to retrieve the confidential background information they have requested and all other background reports requested by the user group.

Access Level 4: Full privileges within the division of the organization. Input and Retrieval of all requests inputted within a specific division of the organization. This level was designed to allow full access to all reports requested by a division.

Access Level 5: Full privileges. Input and Retrieval of all requests input within the entire organization. This level was designed to allow full access to all reports requested by the organization.

Physical Site Security

USAFact's building is secured by lock and key, alarm, and video scanning of the premises. Our Data Center Server Room is locked down and under 24/7 surveillance. Access controls prevent unauthorized entry.

Server Room

The USAFact Server Room is secured by lock and key, monitored by camera and alarm, in addition to continuous monitoring for uptime and climate control.

USAFact computers are all contained in racks and the climate of the room is controlled with a separate cooling system from the remainder of the office. Phone system and computer system are all contained in the same room.

The server room is physically separated from the remainder of the office and only authorized personnel are provided access to that room.

Alarm System

USAFact's building is alarmed by motion detector and intrusion alert. Alarm is sounded and appropriate management personnel are contacted immediately by monitoring center, police are dispatched.

Video Surveillance

There are 16 security cameras that monitor the USAFact facility located both internally and externally. The surrounding activities of the facilities are video taped and stored for auditing purposes.

Summary of Site Security

Building Alarm notifying a secure list of USAFact employees when tripped.

16 Security Cameras surrounding the location with online access to the multiplexer system recording the monitoring of the facility.

Controlled access to network and onsite storage of confidential records filed for reference.

Immediate electronic notification to Network Administrator if systems go offline for any reason such as power outage or equipment failure.

Document Security

File Retention

USAFact archives information as permitted by law and as our customers' needs dictate. Customers may request that data be kept for any length of time within the parameters of the law. Archived background reports are electronically stored and provide our clients with an accessible database for records retention. Data backup is a three tiered process and performed daily. Data is backed up onto tape, CD, and to an electronic storage backup device secured outside the parameters of our server room. Our server room is only accessible to authorized USAFact employees and is kept locked down 24/7.

Documents are stored in-house with secure access. The facility is monitored both internally and externally by a video security surveillance system that tapes the activities within the premises. The facility is also alarmed for motion detection sending the intrusion alert signal directly to a call monitor station in addition to sounding the external alarm. The call monitor station will immediately contact the local police and company personnel.

FACT Act Legislation

The FACT Act Disposal Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to:

- Burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
- Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule.

Data Storage Destruction

Electronically stored data is erased with CIA-standard 21 pass random data overwrite. As hard drives are retired, they are first wiped as above, then physically dismantled, degaussed, drilled, and then securely disposed of.

Document Destruction

All data that is not required to archive is destroyed via a shredding machine located on the premises. Faxes, mail and other paper records are shredded and disposed of in-house on a daily basis. Archived documents are disposed of quarterly on-site by a bonded shredding company under the supervision of USAFact.

Compliance

USAFact complies with all the security requirements of all major legislation regarding the transmission of personal and confidential information. USAFact's compliance procedures include:

1. Use of encryption for all data transmission of personal and/or confidential information;
2. Secure paper document storage with procedures in place for proper disposal of confidential information;
3. Backup procedures to ensure recovery of confidential data in the event of a system's failure;
4. A Disaster Preparedness Plan
5. Penetration and Vulnerability Testing Evaluation from a third party evaluator.
6. Effective Controls are in place for client and employee access to data.

Summary of Data Security Legislation

USAFact has a long history of protecting consumer privacy and our security efforts continue to increase in the electronic age and the evolution of legislation that creates the guidelines we must follow to ensure the security of our data is not compromised.

Sarbanes-Oxley: SOX was enacted to create controls and audits of financial records for publicly traded companies. The legislation created separations of duties within the accounting departments of those companies affected by the legislation. USA-FACT conforms to all data security requirements for SOX, specifically SAS70.

SAS70 (2002): SAS70 audit and subsequent certification is a subsection of Sarbanes-Oxley that ensures the data security and auditing process controls required by legislation is complied with by those companies required to do so. USA -FACT's data infrastructure is regularly tested for security vulnerabilities. Test results are available at your request.

HIPPA (1996): HIPPA covers controls of health care data (medical records). We do not handle any data that is considered part of a medical record (drug screen results are specifically excepted), however, we implement all of the controls HIPPA requires for compliance (access control lists, cryptography and secure paper document storage).

Graham Leach Bliley Act (2001): GLB covers the security and confidentiality of customer records and information, protection from anticipated security threats or unauthorized access to data. We address these concerns with state of the art encryption and SSL protected communications, user access control lists, regular backups, security audits and our disaster recovery plan.

Security Metrics

SecurityMetrics, Inc. is a security corporation certified to perform PCI Scans (ASV), PCI audits (QSA), PABP software audits, penetration tests and forensic analysis. USAFact uses these services to scan its hardware and software security via monthly and annual security sweeps which comply with the penetration testing requirements of the SAS70 subsection of Sarbanes-Oxley. SecurityMetrics provides American Express and many other banks who trust their detailed and thorough security analysis on mission critical data systems.

Data Security Legal Compliance

Disaster Recovery Plan

Over the years, dependence upon the use of computers in the day-to-day business activities of USAFact has increased dramatically as a direct result of the inception of the Internet. Computers now run our business and every vital function of our organization is dependent upon the availability of our network. Therefore it was important for USAFact to develop a strategy to ensure our network and our operations continue to operate in the event of a disaster.

The primary focus of each of the Standard Operating Procedures in USAFact's Disaster Preparedness plan used in the event of a disaster is to fully recover . USAFact's plan contains Standard Operating Procedures (SOP) for the following types of disasters:

Critical Level I	Critical Level II	Critical Level III
Power Outage	Flood	Fire
Bad Weather	Security Breach	Earthquake
Employee Strike		Terrorism
		Severe Weather

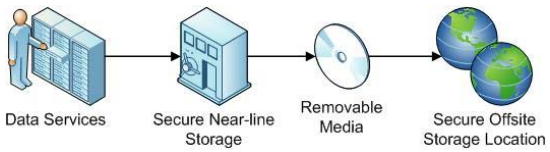
The goal of each SOP is to minimize the amount of data lost and to reduce the amount of downtime experienced by the company in the event of a disaster happening.

Disaster Recovery Basics

USAFact's Disaster Recovery Plan is centered around some basics written into the main body of the plan including:

Backup Data

Backups are sent to a network device for near-line storage which is physically apart from our main operations center and that data is backed up to removable media and stored in a geographically separate location.



Backup Power

USAFact's office building is hooked up to a power generator which can be operational in less than one hour should the building lose power with the ability to operate beyond extended power outages.

Recovery Facility

USAFact has a cold site located approximately 20 miles from the company's main office. The facility is owned by the USAFact's ownership and is sufficient in housing employees and computer systems in the event that a disaster affects the USAFact office. In the event of an isolated incident to our primary building, USAFact has a facility directly next door and can be functional in less than 2 days.

Approved by:	SOP No.:	Issue Date:
USAFact	DP001	October 2003
	Page: 1 of 1	Revised Date: rev. IV: October 2007

Description:

Disaster Preparedness DP001: Recovery from Power Loss Critical Level I

Recovery Time Objective:	1 to 4 hours
Recovery Point Objective:	Full Recovery

Departmental Managers conduct head count, attend to any injured.
Contact responsible parties, clients and vendors.
Turn off all nonessential electronics (faxes, printers, vending machines, air conditioning, workstations, lights). This can also be done, quickly, at the centrally located service panels.
Work with minimal staff (to reduce power drain) until power is restored. Then contact staff to request resumption of work. Ensure all staff signs out with time of departure.
Alert all staff who's shift has not begun to prevent them from arriving.
Ensure the following services are available:
Phone System (can be put in night mode in extreme situations)
Faxes for researchers and clients to utilize
Online retrieval and submission of requests (websrv & raptor)
Automatic services are running (comm01 and autosvcs)
At least one printer, can route all present workers to it.
Establish timeline to power restoration.

Contact Authorities:	Get status report from Riverside Public Utilities commission, 951.782.0330

If less than 1 hour:

Run off UPS devices, post notice on website of possible interruption

If over 1 hour or if 1 hour has passed

Run through Generator Switchover Protocol
Run off generator power. At close of business, if power is restored, switch back to main power. If power is not restored at close of business, shut down all facilities and go through Generator Maintenance Protocol (refill gas, check connections, etc.). Resume generator power at open of business next morning if power has not been restored.

Internet Loss

Initiate T-1 switch-over to back-up data lines.
If all lines are down, switch minimal website hosting to hot site.
If outage persists more than 4 hours, move all servers to hot site, update DNS and function from hot site until main site is recovered.
Notify clients of outage, notify vendors that use our web-based functions, request they fax instead.

Phone System Loss

If outage lasts longer than 1 hour, switch over to traditional phone lines. If outage lasts longer than 4 hours, switch to Centrix voice mail provided by phone company and attempt to route all calls to available personnel.

6200 Box Springs Boulevard
Riverside, California 92507

Tel: 800.547.0263
Fax: 951.656.3336

www.usafact.com

Data Security Summary

USAFact Privacy Statement

USAFact is committed to protecting the confidential information we collect in the performance of our screening services. USAFact utilizes a variety of security technologies and procedures to help protect confidential information from unauthorized access, use, or disclosure. The privacy of the information we collect is preserved by the implementation of four critical control points:

I. Access to Information

To prevent unauthorized access or disclosure, maintain data accuracy, and ensure the appropriate use of information, USAFact has put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we procure for our clients. We take every precaution possible in providing clients secure access to background information. Access is controlled and monitored by several security features in our effort to provide our clients with confidence in our defense against identity theft.

Unless otherwise required by law, only information providers (vendors), USAFact employees, and auditing government entities will be provided access to the consumer information we collect on behalf of our clients and only to the extent needed to perform their duties. USAFact vendors and employees are governed by our privacy policies with respect to the use of this data and are bound by appropriate confidentiality agreements.

II. Authorized Use of Information:

USAFact will not sell, rent, lease or otherwise provide any access to the information we procure for our clients nor will we use or share the consumer information provided to us by our clients or collected by us in the performance of our service in ways unrelated to employment screening.

III. IT Security:

USAFact utilizes a variety of security technologies and procedures to help protect confidential information from unauthorized access, use, or disclosure. For example, we store confidential information on computer systems with limited access, which are located in controlled facilities. When we transmit highly confidential information over the Internet, we protect it through the use of encryption, utilizing Secure Socket Layer (SSL) protocol. USAFact is committed to ensuring the security of your information.

IV. Education/Awareness:

USAFact feels that Education and Awareness are important components of an effective means of maintaining information privacy. Our set up documents for new clients specifically detail the subscriber's responsibility in maintaining confidentiality of the information they contract with USAFact to obtain for their hiring efforts. USAFact describes acceptable and not-acceptable means of electronic dissemination. For the candidates, USAFact developed a consumer awareness web site located on the Internet at reviewmyreport.com. Our consumer web site educates the consumers about the screening process and provides candidates the opportunity to electronically dispute information on their reports.