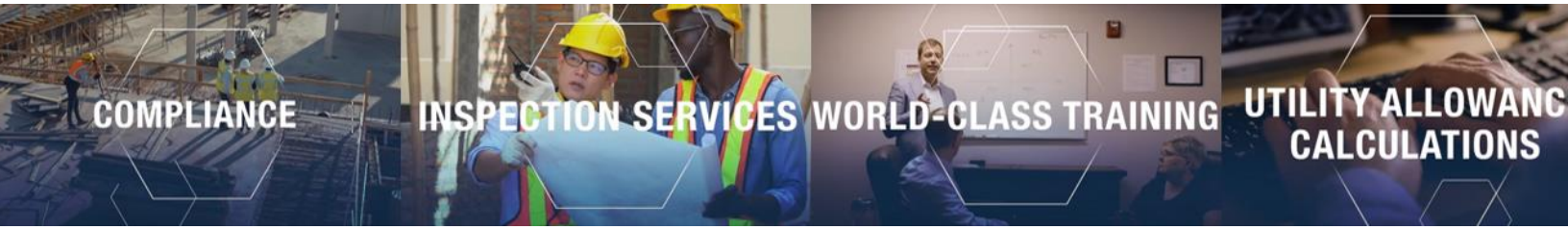
ZEFFERT & ASSOCIATES



Multi-Family Housing Compliance and Training System

Security Policies Overview

2024

www.zeffert.com

Table of Contents

SOC2 4
Functional areas 5
Narrative Summaries 6
BACKUPS, OUTAGES, DISASTER RECOVERY 6
Outages 6
Disaster recovery 6
COMPLIANCE 6
Encryption at rest and in motion 6
PCI 7
Passwords 7
WAF (Web application Firewall) 7
BROWSER ACCESS 7
MONITORING 7
EMAIL 7
SOFTWARE DEVELOPMENT 8
Source code repository. 8
Staging environment. 8
Source reviews. 8
APPLICATION LOGGING 8
VULNERABILITY SCANNING 8
Selected Policies and Procedures 9
APPLICATION SECURITY 10
ASSOCIATE ACCOUNTABILITY POLICY 13
DESKTOP COMPUTING POLICY 18
ENCRYPTION POLICY 23
ASSOCIATE SECURITY PROCEDURES 25
FRAUD & ETHICS POLICY 27
INFORMATION SECURITY MANAGEMENT POLICY 30
RISK ASSESSMENT POLICY 32
VENDOR MANAGEMENT POLICY & PROCEDURES 33

Letter from the Chief Executive Officer

Dear Client,

In our world of multifamily compliance, every detail matters. Handling even routine matters with surgical precision sets us apart as the leader of not only multifamily compliance and training products, but also modern-day technological advancements. The Multi-Family Housing Compliance and Training System is an ecosystem of hardware, software, and online real estate that Zeffert & Associates and Zeffert University utilize for conducting business. This Compliance and Security Overview packet is one way of giving you confidence in our efforts and investments to safeguard your information - including that of residents – so it is always confidential from prying eyes and secure from theft. In fact, this is a serious matter that you should feel empowered to ask of all your vendors.

Some compliance and security highlights include the following.

- ✓ State-of-the-art premises security, including restricted and controlled access to facilities.
- ✓ SOC 2 reporting that evaluates security, integrity, confidentiality, and privacy.
- ✓ Encrypted data at-rest and in end-to-end transmission.
- ✓ Dedicated, multi-redundant servers provide 99.9% uptime.
- ✓ Maintaining robust liability and professional services insurance.

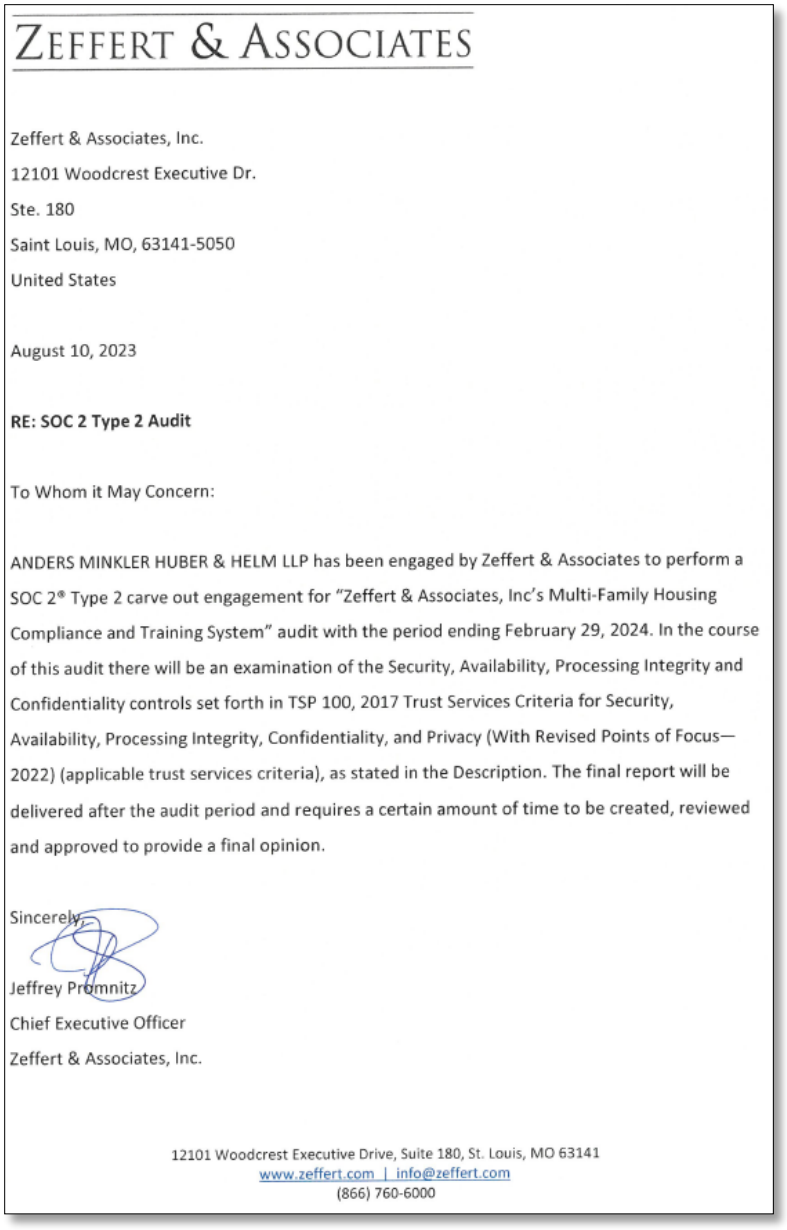
As a mission-driven organization, I thank you for your partnership as we strive to make every community one that families are proud to call home. If you have any questions about our systems and security, please don't hesitate to contact me directly.

Sincerely,

Jeffrey Promnitz
Chief Executive Officer
jpromnitz@zeffert.com

SOC2

SOC 2, or Service Organization Control Type 2, is a cybersecurity compliance framework created by the American Institute of Certified Public Accountants (AICPA). It's standard for service organizations that specifies how they manage customer data. Undergoing this depth of scrutiny is among the clearest demonstrations of commitment to the safety of data. We continue to achieve the highest standards possible and have every intention of remaining the vanguard through continued auditing. Here is a bridge letter demonstrating we will again undergo a voluntary SOC2 audit this year.



ZEFFERT & ASSOCIATES

Zeffert & Associates, Inc.
12101 Woodcrest Executive Dr.
Ste. 180
Saint Louis, MO, 63141-5050
United States

August 10, 2023

RE: SOC 2 Type 2 Audit

To Whom it May Concern:

ANDERS MINKLER HUBER & HELM LLP has been engaged by Zeffert & Associates to perform a SOC 2® Type 2 carve out engagement for "Zeffert & Associates, Inc's Multi-Family Housing Compliance and Training System" audit with the period ending February 29, 2024. In the course of this audit there will be an examination of the Security, Availability, Processing Integrity and Confidentiality controls set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) (applicable trust services criteria), as stated in the Description. The final report will be delivered after the audit period and requires a certain amount of time to be created, reviewed and approved to provide a final opinion.

Sincerely,

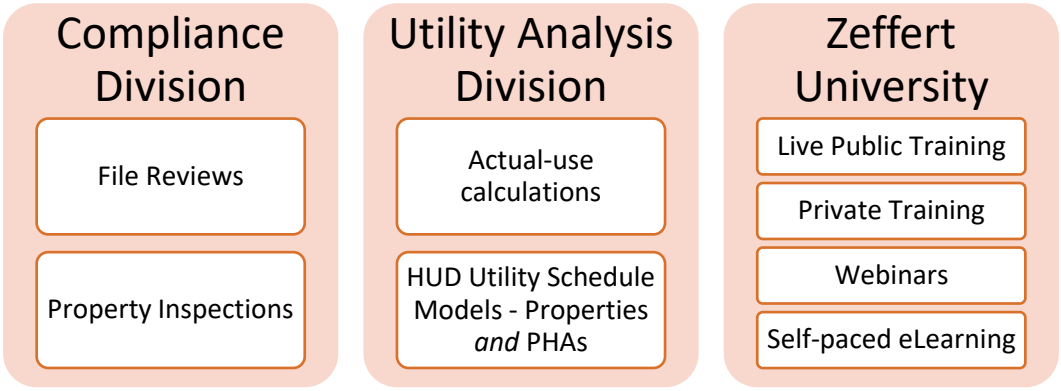
Jeffrey Promnitz
Chief Executive Officer
Zeffert & Associates, Inc.

12101 Woodcrest Executive Drive, Suite 180, St. Louis, MO 63141
www.zeffert.com | info@zeffert.com
(866) 760-6000

Functional areas

Every day of the year, excluding federal holidays, Zeffert is delivering compliance and training products for thousands of multi-family stakeholders all over the country, including the five overseas territories of Puerto Rico, Virgin Islands, Guam, Samoa, and Northern Mariana Islands. This work is heavily concentrated on, but not always limited to, affordable housing projects.

- ✓ Developers
- ✓ Owners
- ✓ Property Managers
- ✓ Housing Finance Agencies
- ✓ Public Housing Authorities
- ✓ Syndicators



Narrative Summaries

Backups, Outages, Disaster Recovery

Each day's operations are fully backed up and securely stored on multiple servers located in separate geographical areas in order to insulate data from environmental disaster.

Outages

Like most companies, we fully embrace and leverage automations and information technology for service delivery enhancements. Because we build in redundancy of all work that is completed every twenty-four hours, should an outage occur, the impact would be minimal. To date, we have never experienced a self-inflicted outage, but we have felt impact from global outages such as when a Google or Amazon Web Services servers experience unanticipated disruption. These affect wide swaths of the map and generally last no more than several minutes.

If an outage occurs, we immediately notify affected clients via electronic communication channels such as email or other agreed-up channel established as a course of routine business. If a global outage were to affect our ability to notify affected clients in a timely manner, then broad social media posts and mass emails would be sent. Details would include, at a minimum, sufficient details that are known of the incident, assurances that data are safe, and the expected cure period.

Disaster recovery

In the event of a disaster, the first step is to secure the environment, then assess the situation, and finally invoke the Recovery Plan. In a worst-case scenario disaster, a full backup can be recovered and deployed within twenty-four to forty-eight hours. In this highly unexpected event, data loss could not exceed more than a twenty-four hour period since data backups are scheduled on that timeline. The client impact would be minimal since it would be restricted to only agreements that include rush order elements or are imminently scheduled for completion.

Compliance

Encryption at rest and in motion

All data are encrypted while at-rest and in-transit when conducted within the Multi-Family Housing Compliance and Training System. This accounts for a significant amount of our work, however, with

field inspectors and trainers, there is also substantial business conducted on a client's premises. Our company Handbook thoroughly covers relevant requirements for safeguarding data in these situations.

PCI

Our products are PCI compliant - ecommerce items such as credit card information are sent directly from the user's browser to the payment gateway over HTTPS and never pass through our servers. We don't store any credit card information in our database.

Passwords

All personal passwords are encrypted and the original passwords are never logged, emailed, or otherwise available. Auto-generated strong passwords (for example, if bulk account creation is used and passwords are omitted) are intentionally not encrypted so that they can be sent to learners via email (this is a common customer requirement). You can configure our system so that this auto-generated password must be replaced on initial login, and the password that is then entered will be stored encrypted.

WAF (Web application Firewall)

We utilize a Web Application Firewall for providing additional protection against things like SQL injection at the app server level.

Browser access

All sites using our default-supplied URLs are served over HTTPS. We encrypt all inbound and outbound traffic using 128-bit TLS/SSL.

Monitoring

Real-time 24/7 monitoring of system components, resources, and security helps to provide signal alerts when issues begin to arise or when subscription renewals are due, for example, so that we are proactive in avoiding threats.

Email

By default, emails are sent using our secure, scalable AWS SES email sending service. Customers have the option of configuring our products to send emails via their own SMTP service. When configured, our products will communicate with the customer's SMTP service using secure TLS and send emails via a single email account used for email sync.

Software Development

Source code repository.

We use a private GitHub repository to store our source code. When an engineer leaves our team, we revoke their GitHub access.

Staging environment.

Code modifications are first deployed and tested in a staging environment. This environment is a duplicate of our production environment and hosted in its own VPN. Once testing is completed, DevOps are notified, and the code is merged into the production branch and deployed to production. If later we find any issues with the deployed changes, we can revert those changes quickly and then redeploy the previous version of the code.

Source reviews.

Before code is deployed to production, it is reviewed by to make sure that the code is clean, well designed, and secure.

Application logging

Every server outputs its logs into its local storage, where it is rotated every 30 days. We do not generate any logs that include sensitive information such as passwords and email communications. We use the Logentries system to provide our support staff with a searchable 30-day running window into our application logs. We install a Logentries agent into each application and job server, and these agents send the log information over HTTPS to Logentries where we can access this information from a user interface.

Vulnerability scanning

Vulnerability scans and penetration testing occur every quarter.

Selected Policies and Procedures

ZEFFERT & ASSOCIATES

Application Security

Category:	Security		Policy #:	8000
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

This policy is to define web application security assessments within Zeffert & Associates. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Zeffert services available both internally and externally as well as satisfy compliance with any relevant policies in place.

Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Zeffert.

Prerequisites

All web application security assessments will be performed by delegated security personnel either employed or contracted by Zeffert. All findings are considered confidential and are to be distributed to people on a "need to know" basis. Distribution of any findings outside of Zeffert is strictly prohibited unless approved by the CFO.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

Policy

Web applications are subject to security assessments based on the following criteria:

- New or Major Application Release — will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- Third Party or Acquired Web Application — will be subject to full assessment after which it will be bound to policy requirements.

- Point Releases — will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- Patch Releases — will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- Emergency Releases — An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the CFO.

All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of medium risk level or greater.

- High — Any high-risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high-risk issues are subject to being taken off-line or denied release into the live environment.
- Medium — Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies limit exposure.
- Low — Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

- Full — A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
- Quick — A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

- Targeted — A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

The current approved web application security assessment tools in use which will be used for testing are:

- Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the CFO.

Policy Compliance

The CFO will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal, and external audits.

Exceptions

Any exception to the policy must be approved by the CFO in advance. An Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Compliance Measurement

The CFO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal, and external audits.

ZEFFERT & ASSOCIATES

Associate Accountability Policy

Category:	Security		Policy #:	8002
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

This policy is to outline the acceptable use of computer equipment at Zeffert & Associates. These rules are in place to protect the Associate and Zeffert. Inappropriate use exposes Zeffert to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Zeffert business or interact with internal networks and business systems, whether owned or leased by Zeffert, the Associate, or a third party. All Associates, contractors, consultants, temporary, and other workers at Zeffert and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Zeffert policies and standards, and local laws and regulation.

This policy applies to Associates, contractors, consultants, temporaries, and other workers at Zeffert, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Zeffert.

Prerequisites

Zeffert proprietary information stored on electronic and computing devices whether owned or leased by Zeffert, the Associate or a third party, remains the sole property of Zeffert. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

Policy

An Associate have a responsibility to promptly report the theft, loss or unauthorized disclosure of Zeffert proprietary information.

An Associate may access, use or share Zeffert proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Associates are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of the Internet/Intranet/Extranet systems. In the absence of such policies, Associates should be guided by departmental policies on personal use, and if there is any uncertainty, Associates should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within Zeffert may monitor equipment, systems, and network traffic at any time, per Infosec's Audit Policy. All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Postings by Associates from a Zeffert email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Zeffert, unless posting is in the course of business duties. Associates must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Associates may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an Associate of Zeffert authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Zeffert-owned resources. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Zeffert.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Zeffert or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting Zeffert business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Zeffert computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Zeffert account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Associate is not an intended recipient or logging into a server or account that the Associate is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the CFO is made.
- Executing any form of network monitoring which will intercept data not intended for the Associate's host unless this activity is a part of the Associate's normal job/duty.
- Circumventing user authentication or security of any host, network or account.

- Introducing honeypots, honeynets, or similar technology on the Zeffert network.
- Interfering with or denying service to any user other than the Associate's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Zeffert Associates to parties outside Zeffert.
-

When using company resources to access and use the Internet, users must realize they represent the company. Whenever Associates state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the CFO.

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies. Use of unsolicited email originating from within Zeffert's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Zeffert or connected via Zeffert's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

Blogging by Associates, whether using Zeffert's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Zeffert's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Zeffert's policy, is not detrimental to Zeffert's best interests, and does not interfere with an Associate's regular work duties. Blogging from Zeffert's systems is also subject to monitoring.

Zeffert's Confidential Information policy also applies to blogging. As such, Associates are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Confidential Information policy when engaged in blogging.

Associates shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Zeffert and/or any of its Associates. Associates are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Zeffert's Non-Discrimination and Anti-Harassment policy.

Associates may also not attribute personal statements, opinions or beliefs to Zeffert when engaged in blogging. If an Associate is expressing his or her beliefs and/or opinions in blogs, the Associate may not, expressly or implicitly, represent themselves as an Associate or representative of Zeffert. Associates assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Zeffert's trademarks, logos and any other Zeffert intellectual property may also not be used in connection with any blogging activity.

Policy Compliance

The CFO will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal, and external audits.

Exceptions

Any exception to the policy must be approved by the CFO in advance. 4.2 Non-Compliance. An Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Compliance Measurement

The CFO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the CFO.

ZEFFERT & ASSOCIATES

Desktop Computing Policy

Category:	Security		Policy #:	8003
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

This policy is to outline the acceptable use of computer equipment at Zeffert. These rules are in place to protect the Associate and Zeffert. Inappropriate use exposes Zeffert to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Zeffert business or interact with internal networks and business systems, whether owned or leased by Zeffert, the Associate, or a third party. All Associates, contractors, consultants, temporary, and other workers at Zeffert and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Zeffert policies and standards, and local laws and regulation.

Prerequisites

Zeffert proprietary information stored on electronic and computing devices whether owned or leased by Zeffert, the Associate or a third party, remains the sole property of Zeffert. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

Policy

You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Zeffert proprietary information. You may access, use or share Zeffert proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Associates are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of the Internet/Intranet/Extranet systems. In the absence of such policies, Associates should be guided by departmental policies on personal use, and if there is any uncertainty, Associates should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within Zeffert may monitor equipment, systems and network traffic at any time, per Audit Policy. Zeffert reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy. System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Unacceptable Use

The following activities are, in general, prohibited. Associates may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an Associate of Zeffert authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Zeffert-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Zeffert.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Zeffert or the end user does not have an active license is strictly prohibited.

- Accessing data, a server or an account for any purpose other than conducting Zeffert business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Zeffert computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Zeffert account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the Associate is not an intended recipient or logging into a server or account that the Associate is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the CFO is made.
- Executing any form of network monitoring which will intercept data not intended for the Associate's host, unless this activity is a part of the Associate's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Zeffert network.
- Interfering with or denying service to any user other than the Associate's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Zeffert Associates to parties outside Zeffert.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever Associates state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Zeffert's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Zeffert or connected via Zeffert's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

Blogging by Associates, whether using Zeffert's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Zeffert's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Zeffert's policy, is not detrimental to Zeffert's best interests, and does not interfere with an Associate's regular work duties. Blogging from Zeffert's systems is also subject to monitoring.

Zeffert's Confidential Information policy also applies to blogging. As such, Associates are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging. Associates shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Zeffert and/or any of its Associates. Associates are also prohibited from making any discriminatory, disparaging,

defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Zeffert's Non-Discrimination and Anti-Harassment policy. Associates may also not attribute personal statements, opinions or beliefs to Zeffert when engaged in blogging. If an Associate is expressing his or her beliefs and/or opinions in blogs, the Associate may not, expressly or implicitly, represent themselves as an Associate or representative of Zeffert. Associates assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Zeffert's trademarks, logos and any other Zeffert intellectual property may also not be used in connection with any blogging activity.

Policy Compliance

The CFO will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the CFO.

Exceptions –

Any exception to the policy must be approved by the CFO in advance. An Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Compliance Measurement

The CFO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the CFO.

ZEFFERT & ASSOCIATES

Encryption Policy

Category:	Security		Policy #:	8004
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

This policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

Scope

This policy applies to all Zeffert Associates and affiliates.

Prerequisites

All Associates should familiarize themselves with the encryption guidelines that follow this introduction.

Policy

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

Hash Function Requirements

In general, Zeffert adheres to the NIST Policy on Hash Functions.

Key Agreement and Authentication

Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH). End points must be authenticated prior to the exchange or derivation of session keys. Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash. All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider. All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

Key Generation

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise. Key generation must be seeded from an industry standard random number generator (RNG).

Policy Compliance

The CFO will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the CFO.

Exceptions

Any exception to the policy must be approved by the CFO in advance. An Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. The CFO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the CFO.

ZEFFERT & ASSOCIATES

Associate Security Procedures

Category:	Security		Policy #:	8005
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

The policy is to provide guidance for secure access to data and facilities, we will be fully implementing the best practices for access security. The goal of Access Management is to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify the assets.

Authorized Users

Zeffert & Associates will have at least one Executive contact and Single Point-of-Contact assigned. They may have as many authorized users as needed.

- Executive Contact - The Executive Contact grants authorized users the right to use a service, while preventing access to non-authorized users. The Executive Contact defines security policies for their account.
- Single Point-of-Contact (SPOC) - Where all day-to-day communications (service updates, maintenance notifications, user access changes) are channeled through. The SPOC grants authorized users the right to use a service, while preventing access to non-authorized users.
- Authorized Users - Authorized users have the right to use a service.
- Emergency Notification Contact Only — Users who only receive notifications from our Emergency Notification System. They do not have an Access Management passcode assigned and are not considered an authorized user (are not approved to request changes to the account).

Access Badge Authorized Users will have physical access to the facility. A Zeffert access agreement form must be signed by all authorized users. Changes to the authorized user access list must be received in writing (email is acceptable) along with their assigned pass code from Executive contact or SPOC. A positive verification request (user access list) will be sent to each SPOC quarterly and must be verified & returned to Zeffert.

Passcode Information

Zeffert will generate a four- or five-digit passcode consisting entirely of numbers which will initially be communicated verbally to each user. A Zeffert proximity badge number will be used as the pass code when applicable. When a service request or remote hands is requested Zeffert Associates will provide assistance only when the passcode has been provided and verified. If the passcode is not provided Zeffert Technical Support will get verification from Executive contact or SPOC.

Physical Security

Visitors with proximity badges will normally have unescorted access to Zeffert. The scanner is the sign-in register for visitors with proximity badges. Associates with a proximity badge may escort their guests, but they must register the guest with the Receptionist. "Tailgating" (Associate lets a guest follow him through an access door) is prohibited by the guest's contract with Zeffert.

When an Associate brings a guest, Zeffert Associates will follow the following process:

- Have them sign in on the sign in sheet.
- Have the guest (first visit only) sign a Zeffert Visitor Access Agreement.
- Issue a visitor badge.

Vendor Access

Vendors will not be granted entrance into the facility without an access form signed by the CFO. In order to remain compliant with our governance procedures it is important that the pass code be documented on the ticket (internal notes only!) and the status be tracked at all times during the life of the ticket.

ZEFFERT & ASSOCIATES

Fraud & Ethics Policy

Category:	Security		Policy #:	8006
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

This policy is to establish a culture of openness, trust and to emphasize the Associate's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every Zeffert Associate.

Scope

This policy applies to Associates, contractors, consultants, temporaries, and other workers at Zeffert, including all personnel affiliated with third parties.

Prerequisites

All Associates should familiarize themselves with the ethics guidelines that follow this introduction.

Executive Commitment to Ethics

Senior leaders and executives within Zeffert must set a prime example. In any business practice, honesty and integrity must be top priority for executives. Executives must have an open-door policy and welcome suggestions and concerns from Associates. This will allow Associates to feel comfortable discussing any issues and will alert executives to concerns within the work force.

Executives must disclose any conflict of interest regarding their position within Zeffert.

Associate Commitment to Ethics

Zeffert Associates will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices. Every Associate needs to apply effort and intelligence in maintaining ethics value. Associates must disclose any conflict of interests regarding their position within Zeffert. Associates will help Zeffert to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries. Associates should consider the following questions to themselves when any behavior is questionable:

- Is the behavior legal?

- Does the behavior comply with all appropriate Zeffert policies?
- Does the behavior reflect Zeffert values and culture?
- Could the behavior adversely affect company stakeholders?
- Would you feel personally concerned if the behavior appeared in a news headline?
- Could the behavior adversely affect Zeffert if all Associates, did it?

Company Awareness

Promotion of ethical conduct within interpersonal communications of Associates will be rewarded. Zeffert will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company. Zeffert will reinforce the importance of the integrity message and the tone will start at the top. Every Associate, manager, director needs to consistently maintain an ethical stance and support ethical behavior. Associates at Zeffert should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

Zeffert has established a best practice disclosure committee to make sure the ethical code is delivered to all Associates and that concerns regarding the code can be addressed.
Associates are required to recertify their compliance to Ethics Policy on an annual basis. 3.5 Unethical Behavior

Zeffert will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications. Zeffert will not tolerate harassment or discrimination.

Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated. Zeffert will not permit impropriety at any time, and we will act ethically and responsibly in accordance with laws. Zeffert Associates will not use corporate assets or business relationships for personal use or gain.

Policy Compliance

The CFO will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the CFO.

Exceptions

Any exception to the policy must be approved by the CFO in advance. 4.2 Non-Compliance. An Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. The CFO will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the CFO.

ZEFFERT & ASSOCIATES

Information Security Management Policy

Category:	Security		Policy #:	8007
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

This policy is to minimize the risk of loss or exposure of sensitive information maintained by Zeffert and to reduce the risk of acquiring malware infections on computers operated by Zeffert.

Scope

This policy covers all computers and servers operating in Zeffert.

Prerequisites

Zeffert staff may only use Zeffert removable media in their work computers. Zeffert removable media may not be connected to or used in computers that are not owned or leased by Zeffert without explicit permission of the Zeffert CFO.

Policy

Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Zeffert Encryption Policy.

Compliance Measurement

The CFO will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the CFO.

Exceptions

Any exception to the policy must be approved by the CFO in advance. An Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Compliance Measurement

The CFO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the CFO.

ZEFFERT & ASSOCIATES

Risk Assessment Policy

Category:	Security		Policy #:	8008
Department:	IT		Effective:	10/01/2023
Executive:	Chief Financial Officer		Prior Version:	10/01/2015

This policy is to empower Infosec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope

To empower Infosec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Prerequisites

The execution, development and implementation of remediation programs is the joint responsibility of CFO and the department responsible for the system area being assessed.

Policy

Associates are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Associates are further expected to work with the Risk Assessment Team in the development of a remediation plan. The CFO will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports and internal and external audits.

Exceptions

Any exception to the policy must be approved by the CFO in advance.

An Associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Compliance Measurement

The CFO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the CFO.

Vendor Management Policy & Procedures

Category:	Information Technology		Policy #:	8010
Department:	Finance		Effective:	07/01/2023
Executive:	Chief Financial Officer		Prior Version:	07/01/2021

The purpose of this policy is to distinguish between critical vendors and vendors that do not provide critical products and services.

Vendor Tier	Security relevance	Example	Measure to safeguard information
Tier 1	Vendor provides **critical services** for organization. Or, the vendor **processes, stores, or has access to sensitive data** (e.g. PII and/or NPI data).	Data Center and IT Service Provider	Review SOC 2 Report or similar report, or review of security assurances
Tier 2	Vendor provides important but non-critical time-sensitive services. Or - in some cases - might have access or might process customer data.	Google (via Google Apps), DropBox, etc. Monitor	Monitor vendor regarding changes and/or sensitive information access.
Tier 3	Vendor is not critical to organization's success and has no access to sensitive information	All others	No special measures

Vendor evaluation:

For Tier 1 and Tier 2 vendors, a vendor evaluation is performed before Zeffert & Associates enters an agreement with the vendor. **For new Tier 1 vendors** - Review SOC 2 Report (or similar) to understand security posture of vendor. Additional risk assessment can be performed (i.e. personal visit, reference check, check public resources for security relevant news or reports about the vendor). **For existing Tier 1 Vendors** - Review SOC 2 Report (or similar) at least once a year for security posture and changes to security posture. New agreements with Tier 1 vendors need to be approved by the CEO after the initial vendor evaluation is performed. **For Tier 2 vendors** - A simplified vendor evaluation is performed before initial contract (review SOC 2 Report or similar if available, review publicly available information regarding security of vendor, i.e. web search).

Contract with Vendors

For tier 1 vendors - Zeffert & Associates attempts to receive contractual assurances regarding vendor's security responsibilities, controls, reporting and performance. If not attainable (standard language in contracts with large service providers), then Zeffert & Associates CEO is informed about contract status with vendor. For other vendors - Standard agreements are used that include privacy and nondisclosure terms and performance agreements, if appropriate.

Jeffrey Promnitz
Chief Executive Officer
National Office
12101 Woodcrest Executive Dr. Suite 180
St. Louis, Missouri 63141

ZEFFERT & ASSOCIATES
ST. LOUIS BUSINESS JOURNAL
BPtW
BEST PLACES TO WORK

"Our Mission is to provide housing compliance and training products that are better and faster than anyone else."