backnine insurance

Acceptable Encryption Policy

1. Overview

See Purpose.

2. Purpose

The purpose of 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.

3. Scope

This policy applies to all BackNine Insurance and Financial Services, Inc. employees and affiliates.

4. Policy

4.1 Algorithm Requirements

4.1.1 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.

4.1.2 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.

4.1.3 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Consider RFC6090 to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

4.2 Hash Function Requirements

In general, BackNine Insurance and Financial Services, Inc. adheres to the NIST Policy on Hash Functions.

4.3 Key Agreement and Authentication

4.3.1 Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

4.3.2 End points must be authenticated prior to the exchange or derivation of session keys.

4.3.3 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.

4.3.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

4.3.5 All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.4 Key Generation

4.4.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

4.4.2 Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5. Policy Compliance

5.1 Compliance Measurement

The BackNine's Security Team team 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 policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the BackNine's Security team in advance.

5.3 Non-Compliance

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

6 Related Standards, Policies and Processes

National Institute of Standards and Technology (NIST) publication FIPS 140-2,

Acceptable Use Policy

6. Overview

BackNine's Security Team's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to BackNine Insurance and Financial Services, Inc.'s established culture of openness, trust and integrity. BackNine's Security Team is committed to protecting BackNine Insurance and Financial Services, Inc.'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of BackNine Insurance and Financial Services, Inc. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every BackNine Insurance and Financial Services, Inc. employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

7. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at BackNine Insurance and Financial Services, Inc. These rules are in place to protect the employee and BackNine Insurance and Financial Services, Inc. Inappropriate use exposes BackNine Insurance and Financial Services, Inc. to risks including virus attacks, compromise of network systems and services, and legal issues.

8. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct BackNine Insurance and Financial Services, Inc. business or interact with internal networks and business systems, whether owned or leased by BackNine Insurance and Financial Services, Inc., the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at BackNine Insurance and Financial Services, Inc. and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with BackNine Insurance and Financial Services, Inc. policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at BackNine Insurance and Financial Services, Inc., including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by BackNine Insurance and Financial Services, Inc.

9. Policy

a. General Use and Ownership

i. BackNine Insurance and Financial Services, Inc. proprietary information stored on electronic and computing devices whether owned or leased by BackNine Insurance and Financial Services, Inc., the employee or a third party, remains the sole property of BackNine Insurance and Financial Services, Inc. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

ii. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of BackNine Insurance and Financial Services, Inc. proprietary information.

iii. You may access, use or share BackNine Insurance and Financial Services, Inc. proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

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

v. For security and network maintenance purposes, authorized individuals within BackNine Insurance and Financial Services, Inc. may monitor equipment, systems and network traffic at any time, per BackNine's Security Team's *Audit Policy*.

vi. BackNine Insurance and Financial Services, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

b. Security and Proprietary Information

i. All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

ii. 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.

iii. 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.

iv. Postings by employees from a BackNine Insurance and Financial Services, Inc. email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of BackNine Insurance and Financial Services, Inc., unless posting is in the course of business duties.

v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

c. Unacceptable Use

The following activities are, in general, prohibited. Employees 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 employee of BackNine Insurance and Financial Services, Inc. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing BackNine Insurance and Financial Services, Inc.-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.

i. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. 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 BackNine Insurance and Financial Services, Inc.

2. 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 BackNine Insurance and Financial Services, Inc. or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting BackNine Insurance and Financial Services, Inc. business, even if you have authorized access, is prohibited.

4. 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.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. 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.

7. Using a BackNine Insurance and Financial Services, Inc. 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.

8. Making fraudulent offers of products, items, or services originating from any BackNine Insurance and Financial Services, Inc. account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee 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.

11. Port scanning or security scanning is expressly prohibited unless prior notification to BackNine's Security Team is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the BackNine Insurance and Financial Services, Inc. network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. 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.

17. Providing information about, or lists of, BackNine Insurance and Financial Services, Inc. employees to parties outside BackNine Insurance and Financial Services, Inc.

ii. Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees 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

1. 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).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. 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.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within BackNine Insurance and Financial Services, Inc.'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by BackNine Insurance and Financial Services, Inc. or connected via BackNine Insurance and Financial Services, Inc.'s network.

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

iii. Blogging and Social Media

1. Blogging by employees, whether using BackNine Insurance and Financial Services, Inc.'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 BackNine Insurance and Financial Services, Inc.'s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate BackNine Insurance and Financial Services, Inc.'s policy, is not detrimental to BackNine Insurance and Financial Services, Inc.'s best interests, and does not interfere with an employee's regular work duties. Blogging from BackNine Insurance and Financial Services, Inc.'s systems is also subject to monitoring.

2. BackNine Insurance and Financial Services, Inc.'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any BackNine Insurance and Financial Services, Inc. confidential or proprietary information, trade secrets or any other material covered by BackNine Insurance and Financial Services, Inc.'s Confidential Information policy when engaged in blogging.

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

4. Employees may also not attribute personal statements, opinions or beliefs to BackNine Insurance and Financial Services, Inc. when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or

implicitly, represent themselves as an employee or representative of BackNine Insurance and Financial Services, Inc. Employees assume any and all risk associated with blogging.

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

10. Policy Compliance

a. Compliance Measurement

BackNine's Security team 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 policy owner.

b. Exceptions

Any exception to the policy must be approved by BackNine's Security Team in advance.

c. Non-Compliance

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

11. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

Clean Desk Policy

Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

12. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

13. Scope

This policy applies to all BackNine Insurance and Financial Services, Inc. employees and affiliates.

14. Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
4.2 Computer workstations must be locked when workspace is unoccupied.
4.3 Computer workstations must be shut completely down at the end of the work day.
4.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
4.7 Laptops must be either locked with a locking cable or locked away in a drawer.
4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
4.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
4.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
4.11 Whiteboards containing Restricted and/or Sensitive information should be erased.
4.12 Lock away portable computing devices such as laptops and tablets.
4.13 Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

15. Policy Compliance

6.1 Compliance Measurement

BackNine's Security Team 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, and feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be approved by BackNine's Security Team in advance.

6.3 Non-Compliance

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

Data Breach Response Policy

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

BackNine Insurance and Financial Services, Inc. Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how BackNine Insurance and Financial Services, Inc.'s established culture of openness, trust and integrity should respond to such activity. BackNine Insurance and Financial Services, Inc. Information Security is committed to protecting BackNine Insurance and Financial Services, Inc.'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of BackNine Insurance and Financial Services, Inc. Protected data or BackNine Insurance and Financial Services, Inc. Sensitive data has occurred must immediately provide a description of what occurred via e-mail to security@back9ins.com, by calling 800-790-1051, or through the use of the help desk reporting web page at http://BackNine Insurance and Financial Services, Inc. This e-mail address, phone number, and web page are monitored by the BackNine Insurance and Financial Services, Inc.'s Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health

Information (PHI) of BackNine Insurance and Financial Services, Inc. members. Any agreements with vendors will contain language similar that protects the fund.

3.0 Policy Confirmed theft, data breach or exposure of BackNine Insurance and Financial Services, Inc. Protected data or BackNine Insurance and Financial Services, Inc. Sensitive data

As soon as a theft, data breach or exposure containing BackNine Insurance and Financial Services, Inc. Protected data or BackNine Insurance and Financial Services, Inc. Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of BackNine Insurance and Financial Services, Inc. data

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by BackNine Insurance and Financial Services, Inc. cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.

Work with BackNine Insurance and Financial Services, Inc. communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

3.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the BackNine Insurance and Financial Services, Inc. community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any BackNine Insurance and Financial Services, Inc. Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the BackNine Insurance and Financial Services, Inc. community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the BackNine Insurance and Financial Services, Inc. community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

4.0 Enforcement

Any BackNine Insurance and Financial Services, Inc. personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

5.0 Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data - See PII and PHI

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

Disaster Recovery Plan Policy

16. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives BackNine Insurance and Financial Services, Inc. a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

17. Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by BackNine Insurance and Financial Services, Inc. that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

18. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

19. Policy

4.1 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

20. Policy Compliance

6.4 Compliance Measurement

BackNine's Security Team 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, and feedback to the policy owner.

6.5 Exceptions

Any exception to the policy must be approved by BackNine's Security Team in advance.

6.6 Non-Compliance

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

backnine insurance

Digital Signature Acceptance Policy

21. Overview

See Purpose.

22. Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in BackNine Insurance and Financial Services, Inc. electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

23. Scope

This policy applies to all BackNine Insurance and Financial Services, Inc. employees and affiliates.

This policy applies to all BackNine Insurance and Financial Services, Inc. employees, contractors, and other agents conducting BackNine Insurance and Financial Services, Inc. business with a BackNine Insurance and Financial Services, Inc.-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-BackNine Insurance and Financial Services, Inc. affiliated persons or organizations.

24. Policy

A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted on the site of the Chief Financial Officer (CFO) on the organization's intranet.

The CFO's office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

4.1 Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

4.2 Signer Responsibilities

4.2.1 Signers must obtain a signing key pair from BackNine's Security Team. This key pair will be generated using BackNine Insurance and Financial Services, Inc.'s Public Key Infrastructure (PKI) and the public key will be signed by the BackNine Insurance and Financial Services, Inc.'s Certificate Authority (CA).

4.2.2 Signers must sign documents and correspondence using software approved by BackNine Insurance and Financial Services, Inc. IT organization.
4.2.3 Signers must protect their private key and keep it secret.
4.2.4 If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact BackNine Insurance and Financial Services, Inc. Identity Management Group immediately to have the signer's digital key pair revoked.

4.3 Recipient Responsibilities
4.3.1 Recipients must read documents and correspondence using software approved by BackNine Insurance and Financial Services, Inc. IT department.
4.3.2 Recipients must verify that the signer's public key was signed by the BackNine Insurance and Financial Services, Inc.'s Certificate Authority (CA) by viewing the details about the signed key using the software they are using to read the document or correspondence.
4.3.3 If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.
4.3.4 If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to BackNine Insurance and Financial Services, Inc. Identity Management Group.

25. Policy Compliance

6.7 Compliance Measurement
BackNine's Security Team 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 policy owner.

6.8 Exceptions
Any exception to the policy must be approved by BackNine's Security Team in advance.

6.9 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7 Related Standards, Policies and Processes

None.

8 References

Note that these references were used only as guidance in the creation of this policy template. We highly recommend that you consult with your organization's legal counsel, since there may be federal, state, or local regulations to which you must comply. Any other PKI-related policies your organization has may also be cited here.

American Bar Association (ABA) Digital Signature Guidelines
http://www.abanet.org/scitech/ec/isc/dsgfree.html

Minnesota State Agency Digital Signature Implementation and Use
http://mn.gov/oet/policies-and-standards/business/policy-pages/standard_digital_signature.jsp

Minnesota Electronic Authentication Act
https://www.revisor.leg.state.mn.us/statutes/?id=325K&view=chapter_-stat.325K.001

City of Albuquerque E-Mail Encryption / Digital Signature Policy
http://mesa.cabq.gov/policy.nsf/WebApprovedX/4D4D4667D0A7953A87256E7B004F6720?OpenDocument

West Virginia Code §39A-3-2: Acceptance of electronic signature by governmental entities in satisfaction of signature requirement.
http://law.justia.com/westvirginia/codes/39a/wvc39a-3-2.html

Email Policy

Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

Purpose

The purpose of this email policy is to ensure the proper use of BackNine Insurance and Financial Services, Inc. email system and make users aware of what BackNine Insurance and Financial Services, Inc. deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within BackNine Insurance and Financial Services, Inc. Network.

Scope

This policy covers appropriate use of any email sent from a BackNine Insurance and Financial Services, Inc. email address and applies to all employees, vendors, and agents operating on behalf of BackNine Insurance and Financial Services, Inc.

Policy

4.1 All use of email must be consistent with BackNine Insurance and Financial Services, Inc. policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.2 BackNine Insurance and Financial Services, Inc. email account should be used primarily for BackNine Insurance and Financial Services, Inc. business-related purposes; personal communication is permitted on a limited basis, but non-BackNine Insurance and Financial Services, Inc. related commercial uses are prohibited.

4.3 All BackNine Insurance and Financial Services, Inc. data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.

4.4 Email should be retained only if it qualifies as a BackNine Insurance and Financial Services, Inc. business record. Email is a BackNine Insurance and Financial Services, Inc. business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

4.5 Email that is identified as a BackNine Insurance and Financial Services, Inc. business record shall be retained according to BackNine Insurance and Financial Services, Inc. Record Retention Schedule.

4.6 The BackNine Insurance and Financial Services, Inc. email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any BackNine Insurance and Financial Services, Inc. employee should report the matter to their supervisor immediately.

4.7 Users are prohibited from automatically forwarding BackNine Insurance and Financial Services, Inc. email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain BackNine Insurance and Financial Services, Inc. confidential or above information.

4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct BackNine Insurance and Financial Services, Inc. business, to create or memorialize any binding transactions, or to store or retain email on behalf of BackNine Insurance and Financial Services, Inc. Such communications and transactions should be conducted through proper channels using BackNine Insurance and Financial Services, Inc.-approved documentation.

4.9 Using a reasonable amount of BackNine Insurance and Financial Services, Inc. resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a BackNine Insurance and Financial Services, Inc. email account is prohibited.

4.10 BackNine Insurance and Financial Services, Inc. employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

4.11 BackNine Insurance and Financial Services, Inc. may monitor messages without prior notice. BackNine Insurance and Financial Services, Inc. is not obliged to monitor email messages.

Policy Compliance

8.1 Compliance Measurement

BackNine's Security Team 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, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by BackNine's Security Team in advance.

8.3 Non-Compliance

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

Ethics Policy

26. Overview

BackNine Insurance and Financial Services, Inc. is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When BackNine Insurance and Financial Services, Inc. addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

BackNine Insurance and Financial Services, Inc. will not tolerate any wrongdoing or impropriety at any time. BackNine Insurance and Financial Services, Inc. will take the appropriate measures act quickly in correcting the issue if the ethical code is broken.

27. Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee'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 BackNine Insurance and Financial Services, Inc. employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

28. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at BackNine Insurance and Financial Services, Inc., including all personnel affiliated with third parties.

29. Policy

4.1 Executive Commitment to Ethics

4.1.1 Senior leaders and executives within BackNine Insurance and Financial Services, Inc. must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

4.1.2 Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

4.1.3 Executives must disclose any conflict of interests regard their position within BackNine Insurance and Financial Services, Inc.

4.2 Employee Commitment to Ethics

4.2.1 BackNine Insurance and Financial Services, Inc. employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

4.2.2 Every employee needs to apply effort and intelligence in maintaining ethics value.

4.2.3 Employees must disclose any conflict of interests regard their position within BackNine Insurance and Financial Services, Inc.

4.2.4 Employees will help BackNine Insurance and Financial Services, Inc. to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

4.2.5 Employees should consider the following questions to themselves when any behavior is questionable:

- Is the behavior legal?
- Does the behavior comply with all appropriate BackNine Insurance and Financial Services, Inc. policies?
- Does the behavior reflect BackNine Insurance and Financial Services, Inc. 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 BackNine Insurance and Financial Services, Inc. if all employees did it?

4.3 Company Awareness

4.3.1 Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

4.3.2 BackNine Insurance and Financial Services, Inc. will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4 Maintaining Ethical Practices

4.4.1 BackNine Insurance and Financial Services, Inc. will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

4.4.2 Employees at BackNine Insurance and Financial Services, Inc. should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.4.3 BackNine Insurance and Financial Services, Inc. has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.4.4 Employees are required to recertify their compliance to Ethics Policy on an annual basis.

4.5 Unethical Behavior

4.5.1 BackNine Insurance and Financial Services, Inc. will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.5.2 BackNine Insurance and Financial Services, Inc. will not tolerate harassment or discrimination.

4.5.3 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.

4.5.4 BackNine Insurance and Financial Services, Inc. will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

4.5.5 BackNine Insurance and Financial Services, Inc. employees will not use corporate assets or business relationships for personal use or gain.

30. Policy Compliance

8.4 Compliance Measurement

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

8.5 Exceptions

None.

8.6 Non-Compliance

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

Pandemic Response Planning Policy

This policy is intended for companies that do not meet the definition of critical infrastructure as defined by the federal government. This type of organization may be requested by public health officials to close their offices to non-essential personnel or completely during a worst-case scenario pandemic to limit the spread of the disease. Many companies would run out of cash and be forced to go out of business after several weeks of everyone not working. Therefore, developing a response plan in advance that addresses who can work remotely, how they will work and identifies what other issues may be faced will help the organization survive at a time when most people will be concerned about themselves and their families.

Disasters typically happen in one geographic area. A hurricane or earthquake can cause massive damage in one area, yet the worst damage is usually contained within a few hundred miles. A global pandemic, such as the 1918 influenza outbreak which infected 1/3 of the world's population, cannot be dealt with by failing over to a backup data center. Therefore, additional planning steps for IT architecture, situational awareness, employee training and other preparations are required.

31. Purpose

This document directs planning, preparation and exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process. The objective is to address the reality that pandemic events can create personnel and technology issues outside the scope of the traditional DR/BCP planning process as potentially 25% or more of the workforce may be unable to come to work for health or personal reasons.

32. Scope

The planning process will include personnel involved in the business continuity and disaster recovery process, enterprise architects and senior management of BackNine Insurance and Financial Services, Inc. During the implementation of the plan, all employees and contractors will need to undergo training before and during a pandemic disease outbreak.

33. Policy

BackNine Insurance and Financial Services, Inc. will authorize, develop and maintain a Pandemic Response Plan addressing the following areas:

4.1 The Pandemic Response Plan leadership will be identified as a small team which will oversee the creation and updates of the plan. The leadership will also be responsible for developing internal expertise on the transmission of diseases and other areas such as second wave phenomenon to guide planning and response efforts. However, as with any other critical position, the leadership must have trained alternates that can execute the plan should the leadership become unavailable due to illness.

4.2 The creation of a communications plan before and during an outbreak that accounts for congested telecommunications services.

4.3 An alert system based on monitoring of World Health Organization (WHO) and other local sources of information on the risk of a pandemic disease outbreak.

4.4 A predefined set of emergency polices that will preempt normal BackNine Insurance and Financial Services, Inc. policies for the duration of a declared pandemic. These polices are to be organized into different levels of response that match the level of business disruption expected from a possible pandemic disease outbreak within the community. These policies should address all tasks critical to the continuation of the company including:

a) How people will be paid
b) Where they will work – including staying home with or bringing kids to work.
c) How they will accomplish their tasks if they cannot get to the office

4.5 A set of indicators to management that will aid them in selecting an appropriate level of response bringing into effect the related policies discussed in section 4.4—for the organization. There should be a graduated level of response related to the WHO pandemic alert level or other local indicators of a disease outbreak.

4.6 An employee training process covering personal protection including:

a) Identifying symptoms of exposure
b) The concept of disease clusters in day cares, schools or other gathering places
c) Basic prevention - limiting contact closer than 6 feet, cover your cough, hand washing
d) When to stay home
e) Avoiding travel to areas with high infection rates

4.7 A process for the identification of employees with first responders or medical personnel in their household. These people, along with single parents, have a higher likelihood of unavailability due to illness or child care issues.

4.8 A process to identify key personnel for each critical business function and transition their duties to others in the event they become ill.

4.9 A list of supplies to be kept on hand or pre-contracted for supply, such as face masks, hand sanitizer, fuel, food and water.

4.10 IT related issues:

a) Ensure enterprise architects are including pandemic contingency in planning
b) Verification of the ability for significantly increased telecommuting including bandwidth, VPN concentrator capacity/licensing, ability to offer voice over IP and laptop/remote desktop availability
c) Increased use of virtual meeting tools – video conference and desktop sharing
d) Identify what tasks cannot be done remotely
e) Plan for how customers will interact with the organization in different ways

4.11 The creation of exercises to test the plan.

4.12 The process and frequency of plan updates at least annually.

4.13 Guidance for auditors indicating that any review of the business continuity plan or enterprise architecture should assess whether they appropriately address the BackNine Insurance and Financial Services, Inc. Pandemic Response Plan.

34. Policy Compliance

8.7 Compliance Measurement

BackNine's Security Team 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, and feedback to the policy owner.

8.8 Exceptions
Any exception to the policy must be approved by BackNine's Security Team in advance.

8.9 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9 Related Standards, Policies and Processes

World Health Organization

Password Construction Guidelines

35. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

36. Purpose

The purpose of this guidelines is to provide best practices for the created of strong passwords.

37. Scope

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

38. Statement of Guidelines

Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of 'password manager' software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

39. Policy Compliance

9.1 Compliance Measurement

BackNine's Security Team 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, and feedback to the policy owner.

9.2 Exceptions

Any exception to the policy must be approved by BackNine's Security Team in advance.

9.3 Non-Compliance

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

Password Protection Policy

40. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to BackNine Insurance and Financial Services, Inc. systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

41. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

42. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any BackNine Insurance and Financial Services, Inc. facility, has access to the BackNine Insurance and Financial Services, Inc. network, or stores any non-public BackNine Insurance and Financial Services, Inc. information.

43. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.

4.1.3 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommend that some form of multi-factor authentication is used for any privileged accounts

4.2 Password Change

4.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.

4.2.2 Password cracking or guessing may be performed on a periodic or random basis by BackNine's Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential BackNine Insurance and Financial Services, Inc. information. Corporate Information Security recognizes that legacy

applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.3 Passwords may be stored only in “password managers” authorized by the organization.

4.3.4 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.5 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Multi-Factor Authentication

4.5.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

44. Policy Compliance

9.4 Compliance Measurement

BackNine’s Security Team 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, and feedback to the policy owner.

9.5 Exceptions

Any exception to the policy must be approved by BackNine’s Security Team in advance.

9.6 Non-Compliance

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

10 Related Standards, Policies and Processes

- Password Construction Guidelines

backnine insurance

Security Response Plan Policy

45. Overview

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

46. Purpose

The purpose of this policy is to establish the requirement that all business units supported by BackNine's Security Team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

47. Scope

This policy applies any established and defined business unity or entity within the BackNine Insurance and Financial Services, Inc.

Policy

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with BackNine's Security Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with BackNine's Security Team in the development and maintenance of a Security Response Plan.

4.1 Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2 Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

4.3 Triage
The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4 Identified Mitigations and Testing
The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5 Mitigation and Remediation Timelines
The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5 Policy Compliance

5.1 Compliance Measurement
Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2 Exceptions
Any exception to this policy must be approved by BackNine's Security Team in advance and have a written record.

5.3 Non-Compliance
Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP

End User Encryption Key Protection Policy

48. Overview

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys use to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

49. Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

50. Scope

This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

- encryption keys issued by BackNine Insurance and Financial Services, Inc.
- encryption keys used for BackNine Insurance and Financial Services, Inc. business
- encryption keys used to protect data owned by BackNine Insurance and Financial Services, Inc.

The public keys contained in digital certificates are specifically exempted from this policy.

51. Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

4.1 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in BackNine Insurance and Financial Services, Inc.'s *Acceptable Encryption Policy.* If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

4.2 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

4.2.1 BackNine Insurance and Financial Services, Inc.'s Public Key Infrastructure (PKI) Keys

The public-private key pairs used by the BackNine Insurance and Financial Services, Inc.'s public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents BackNine's Security Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with
BackNine Insurance and Financial Services, Inc. policies.

Access to the private keys stored on a BackNine Insurance and Financial Services, Inc.issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

4.2.2 Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the requirements for protecting the private keys are the same as those for private keys associated with BackNine Insurance and Financial Services, Inc.'s PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.

BackNine's Security Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with BackNine Insurance and Financial Services, Inc. *Password Policy*. BackNine's Security Team's representatives will store and protect the escrowed keys as described in the BackNine Insurance and Financial Services, Inc. *Certificate Practice Statement Policy.*

4.2.2.1 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

4.2.2.2 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

4.3 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in BackNine Insurance and Financial Services, Inc.'s *Physical Security policy*, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

4.4 Personal Identification Numbers (PINs), Passwords and Passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in BackNine Insurance and Financial Services, Inc.'s *Password Policy.*

4.5 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to BackNine's Security Team. BackNine's Security Team's personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

52. Policy Compliance

10.1 Compliance Measurement

BackNine's Security Team 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, and feedback to the policy owner.

10.2 Exceptions

Any exception to the policy must be approved by BackNine's Security Team in advance.

10.3 Non-Compliance

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

11 Related Standards, Policies and Processes

- Acceptable Encryption Policy
- Certificate Practice Statement Policy
- Password Policy
- Physical Security policy

12 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Certificate authority (CA)
- Digital certificate
- Digital signature
- Key escrow
- Plaintext
- Public key cryptography
- Public key pairs
- Symmetric cryptography