UNISHKA
Research Service

Internet, Email, and Cyber Security Policy

January 2017

FOREWORD

The following manual is intended to provide an overview of the Internet, Email, and Cyber Security Policy for UNISHKA Research Service, LLC (UNISHKA). Its primary purpose is to formalize policies relating to electronic media and communications.

All UNISHKA staff members are bound by the policies. Any unauthorized deviation from these policies and procedures is prohibited and may result in disciplinary action or termination.

The effective date of all policies described in this manual is January 1, 2017. If a policy is added or modified subsequent to this date, the effective date of the new/revised policy will be indicated within the policy heading.

Finally, we welcome your comments or suggestions for improvements and these may be incorporated in future revisions of these procedures.

Jeffrey Coonjohn 1 January 2017
CEO & Chief Operations Officer
UNISHKA Research Service, LLC

Contents

1 ACCEPTABLE USE POLICY

1.1 Overview

UNISHKA is committed to protecting its employees, consultants, partners, clients and the company within the virtual workspace. Effective security is a team effort involving the participation and support of every UNISHKA 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.

1.2 Purpose

The purpose of this policy is to outline the acceptable use of UNISHKA's computers and electronic systems. These rules are in place to protect the employee and UNISHKA from unnecessary risk. Inappropriate use of computers or electronic systems exposes UNISHKA to risks including virus attacks, compromise of network systems as well as potential legal issues.

1.3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources used to conduct UNISHKA business or interact with internal networks or business systems, whether owned or leased by UNISHKA, the employee, or a third party. All employees, contractors, consultants and other workers, both temporary and full-time, at UNISHKA and its subsidiaries are responsible for exercising constant good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with all UNISHKA's policies and standards, in addition to local laws and regulations. Exceptions to this policy must be authorized in writing by senior management. This policy applies to all employees, contractors, consultants, and other workers, both temporary and full-time at UNISHKA and its subsidiaries (collectively referred to as "employees"). This includes all personnel affiliated with third parties. This policy also applies to all equipment and property that is owned or leased by UNISHKA.

1.4 General Use and Ownership

- All UNISHKA's proprietary information stored on electronic and computing devices whether owned or leased by UNISHKA, the employee or a third party, remains the sole property of UNISHKA.

You must ensure through legal or technical means that proprietary information is protected.

- You have an obligation to report the theft, loss or unauthorized disclosure of any of UNISHKA's proprietary information.
- You may access, use or share UNISHKA's proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- 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.
- For security and network maintenance purposes, authorized individuals within UNISHKA may monitor equipment, systems and network traffic at any time.
- UNISHKA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.5 Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with this policy.
- System level and user level passwords must comply with the *Password Protection Policy* (Found at the end of this manual). Providing access to another individual, either deliberately or through failure to secure its access, requires an exception to policy and senior management approval.
- 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 employees from a UNISHKA email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UNISHKA, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

1.6 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 UNISHKA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UNISHKA-owned resources.

The lists below are by no means exhaustive, but are an attempt to provide a framework for activities which fall into the category of unacceptable use.

1.7 System and Network Activities

The following activities are prohibited without specific written authorization from senior management:

- 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 UNISHKA.
- 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 UNISHKA or the end user does not have an active license.
- 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 without authorization. This includes family and other household members when work is being done at home.
- Using a UNISHKA computing asset to transmit 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 UNISHKA 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 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.

- Port scanning or security scanning is prohibited unless prior notification to UNISHKA is made.
- 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.
- Introducing honeypots, honeynets, or similar technology on the UNISHKA network.
- Interfering with or denying service to any user other than the employee’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 including, but not limited to, finances, company and/or personal security, company projects (past, current, and future), or lists of UNISHKA employees to parties outside UNISHKA, unless these duties are within the scope of regular duties. The appropriate management should be consulted prior to export of any material that is in question.

1.8 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. As above, the following activities are prohibited without specific written authorization from senior management:

- Sending unsolicited “junk mail” or other advertising material to individuals who did not specifically request such material unless this activity is a part of the employee’s assigned job/duty.
- Any form of harassment via email, telephone or paging, whether through language, frequency or size of messages. Any employee who feels they’ve been the target of harassment should forward the correspondence in question to the HR Department and/or their direct supervisor. Furthermore, the employee should retain these emails for their personal records.

- Unauthorized use or forging of email header information, as well as misuse of UNISHKA templates.
- 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.

1.9 Blogging and Social Media

- Blogging by employees, whether using UNISHKA's property, systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of UNISHKA's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate UNISHKA's policy, is not detrimental to UNISHKA's best interests, and does not interfere with an employee's regular work duties. Blogging from UNISHKA's systems is also subject to monitoring.
- UNISHKA's *Confidential Information Policy* (see below) also applies to blogging. As such, employees are prohibited from revealing any of UNISHKA's confidential or proprietary information, trade secrets or any other material covered by UNISHKA's Confidential Information policy when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of UNISHKA 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 UNISHKA's *Non-Discrimination and Anti-Harassment policy* (see UNISHKA's Employee Manual).
- Employees may also not attribute personal statements, opinions or beliefs to UNISHKA 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 UNISHKA. Employees 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, UNISHKA's trademarks, logos and any other of UNISHKA's intellectual property may also not be used regarding any blogging activity.

2 CLEAN DESK POLICY

2.1 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.

2.2 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.

2.3 Scope

This policy applies to all UNISHKA employees and affiliates.

2.4 Policy

- 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.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted, Confidential 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.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left unattended.

- All portables including, but not limited to, Laptops, Tablets, etc. must be either locked with a locking cable or locked away in a drawer.
- 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. A designated UNISHKA employee will maintain a password journal as part of the company's emergency or succession planning.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

2.5 Digital Signature Acceptance Policy

UNISHKA does not currently use Digital Signatures.

3 DISASTER RECOVERY PLAN POLICY

3.1 Overview

It is important to realize that having a contingency plan in the event of a disaster gives UNISHKA 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.

3.2 Purpose

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

3.3 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.

3.4 Policy

3.4.1 Contingency Plans:

The following contingency plans must be created and stored in binders at each UNISHKA office:

- **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 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. Copy of data stored on electronic systems (i.e. SharePoint) should be backed-up not less than once per month on an external hard drive.

- **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.

4 EMAIL POLICY

4.1 Overview

Electronic email is pervasively used in almost all aspects of UNISHKA operations 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.

4.2 Purpose

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

4.3 Scope

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

4.4 Policy

- All use of email must be consistent with UNISHKA policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- UNISHKA email accounts should be used primarily for UNISHKA business-related purposes; personal communication is permitted on a limited basis, but non-UNISHKA related commercial uses are prohibited.
- All UNISHKA data contained within an email message or an attachment must be secured.
- Emails should be retained in accordance with the UNISHKA Record Retention Schedule. Email is a UNISHKA business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- The UNISHKA email system should not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, personal appearance features, disabilities, age, sexual orientation, pornography, religious beliefs and practice,

political beliefs, or national origin. Employees who receive any emails with this content from any UNISHKA employee should report the matter to UNISHKA's HR Department or their supervisor immediately.

- Users are prohibited from automatically forwarding UNISHKA email to a third-party email system without supervisory permission. Individual messages which are forwarded by the user must not contain UNISHKA confidential or above information.
- Unless required by special circumstance, users should refrain from using third-party email systems and storage servers such as Google, Yahoo, Hotmail etc. to conduct UNISHKA business, to create or memorialize any binding transactions, or to store or retain email on behalf of UNISHKA. Such communications and transactions should be conducted through proper channels using UNISHKA-approved documentation.
- Using a reasonable amount of UNISHKA resources for personal emails is acceptable, but non-work-related email should be saved in a separate folder from work related email. Sending chain letter emails from a UNISHKA email account is prohibited.
- UNISHKA employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- UNISHKA may monitor messages without prior notice. UNISHKA is not obliged to monitor email messages.

5 ETHICS POLICY

5.1 Overview

UNISHKA is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When UNISHKA addresses issues proactively and uses correct judgment, it will help set us apart from competitors. UNISHKA will not tolerate any unethical behavior. UNISHKA will take the appropriate measures to act quickly in correcting the issue if there is a breach in the Ethics Policy or Code of Conduct.

5.2 Purpose

The purpose of this policy is to establish a culture of openness and trust and to emphasize the employee's and client's expectation to be treated to fair business practices. This policy will serve to guide business behavior and to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every UNISHKA employee. All employees should familiarize themselves with the ethics and guidelines that follow this introduction.

5.3 Scope

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

5.4 Policy

5.4.1 Executive Commitment to Ethics:

- Senior leaders and executives within UNISHKA 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 employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.
- Executives must disclose any conflict of interests regard their position within UNISHKA.

5.4.2 Employee Commitment to Ethics:

- UNISHKA employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
- Every employee needs to apply effort and intelligence in maintaining ethical values.
- Employees must disclose any conflict of interests regard their position within UNISHKA.
- Employees should consider the following questions to themselves when any behavior is questionable:
  - Is the behavior legal?
  - Does the behavior comply with all appropriate UNISHKA policies?
  - Does the behavior reflect UNISHKA 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 UNISHKA if all employees, did it?

5.4.3 Company Awareness:

- Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- UNISHKA will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

5.4.4 Maintaining Ethical Practices:

- UNISHKA will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs to consistently maintain an ethical stance and support ethical behavior.
- Employees at UNISHKA should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
- UNISHKA 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.
- Employees are required to recertify their compliance to UNISHKA’s Code of Conduct on a routine basis.

5.4.5 Unethical Behavior

- UNISHKA will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
- UNISHKA 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.
- UNISHKA will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
- UNISHKA employees will not use corporate assets or business relationships for personal use or gain.

6 PASSWORD POLICY

6.1 Password Construction Guidelines

6.1.1 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 the network. This guideline provides best practices for creating secure passwords.

6.1.2 Purpose

The purpose of this guideline is to provide best practices for the creation of strong passwords.

6.1.3 Scope

This guideline applies to employees, contractors, consultants, temporary and other workers at UNISHKA, 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.

6.1.4 Policy

All passwords should meet or exceed the following guidelines:

- Contain at least 7 alphanumeric characters.
- Contain both upper and lower-case letters.
- Contain at least one number (For example, 0-9).
- Contain at least one special character (For example, !$%^&*()_+|~-=\`{}[]:”;’<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

Never Write Down a Password:
Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R!

Passphrases:
Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

6.2 Password Protection Policy

6.2.1 Overview

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

6.2.2 Purpose

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

6.2.3 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 UNISHKA facility, has access to the UNISHKA network, or stores any non-public UNISHKA information.

6.2.4 Policy

Password Creation:

- All user-level and system-level passwords must conform to the Password Construction Guidelines.
- Users must not use the same password for UNISHKA accounts as for other non-UNISHKA access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various UNISHKA access needs.

Password Change:

- All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
- All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months.
- Password cracking or guessing may be performed on a periodic or random basis by UNISHKA 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.

Password Protection:

- Passwords should not be shared with anyone (except for the Company Password Journal which is necessary for Emergency Response and Succession Planning). All passwords are to be treated as Confidential UNISHKA information.
- Passwords should not be inserted into email messages.
- Passwords should not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share UNISHKA passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members except in accordance with Company policy.
- Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

7 CONFIDENTIAL INFORMATION ELECTRONIC PROTECTION POLICY

7.1 Overview

Confidential information stored on the UNISHKA network is an important resource for all UNISHKA employees and those acting on behalf of the UNISHKA in performing their job duties. As the organization has grown, so too have internal and external threats to the security and confidentiality of UNISHKA information.

Maintaining the integrity of UNISHKA Confidential Information is of utmost importance to the organization. In response, the UNISHKA developed this policy to reduce the risk of compromising confidential UNISHKA information and to comply with applicable state and federal laws, Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Americans with Disabilities Act (ADA) of 1990. In addition, the UNISHKA's Code of Conduct emphasizes the organization's commitment to operating in an ethical, honest, and lawful manner.

7.2 Policy

All UNISHKA employees and those acting on behalf of the UNISHKA who have access to confidential UNISHKA information will ensure that this information is treated in accordance with the "Requirements for Maintaining Confidential Information" (found below in this document).

In addition, all UNISHKA employees and those acting on behalf of the UNISHKA are responsible for immediately reporting any suspected violation(s) of this policy or any other action which violates confidentiality of UNISHKA information to his or her supervisor or Director of Business Administration.

7.2.1 Definitions

For purposes of this policy, the following are definitions that will assist employees and those acting on behalf of the UNISHKA in understanding and ensuring compliance with the policy:

Information is defined as any communication or reception of knowledge regarding the UNISHKA and includes facts, data, or opinions that may consist of numerical, graphic, or narrative forms, whether oral, downloaded to equipment, or maintained in mediums, including, but not limited to, computerized databases, papers, microfilms, magnetic tapes, disks, CDs, flash drives, and cell phones.

Confidential Information is defined as any UNISHKA Information as described above that specifically identifies and/or describes an employee, an employee's protected health information, UNISHKA operations (including identifying countries in which we work if that is not otherwise identified on the UNISHKA website) and/or UNISHKA organizational information, which if disclosed or released, a reasonable person would conclude that negative financial, competitive, or productive loss may occur and/or may cause legal or other non-beneficial impacts on the UNISHKA.

Examples of Confidential Information

Additional specific examples of Confidential Information include, but are not limited to, the following items. Individuals who are uncertain if the type of information being used is confidential should seek clarification from their manager/supervisor.

- an employee's name, birth date, race, gender, marital status, disability status, veteran status, citizenship, Social Security number (SSN)
- an employee's home address, home telephone number(s), relatives' names, addresses, and telephone numbers
- an employee's Personnel File
- an employee's employment status, including leave of absence information, appointment begin and end dates, termination date, termination reason
- an employee's payroll information, including salary rates, tax information, withholdings, direct deposit information
- an employee's benefit enrollment information
- an employee's Protected Health Information (PHI)
- organizational finance information
- organizational operating plans, including strategic, business, and marketing plans
- organizational operating environments (i.e. locations and/or target participants)
- facilities management documentation, including security system information
- auditing information, including internal audit reports and investigative records
- all organizational legal documents, including pending lawsuits and attorney-client communications

Requirements for Maintaining Confidential Information

All UNISHKA employees and those acting on behalf of the UNISHKA with authorized access to Confidential Information stored on the UNISHKA network or in any media format, are required to protect this information. All UNISHKA employees and those acting on behalf of the UNISHKA:

- will access Confidential Information for the sole purpose of performing their job-related duties.
- will not seek personal benefit or permit others to benefit personally from any Confidential Information that comes to them through their work assignments.
- will not permit unauthorized use of any Confidential Information that can be found on the UNISHKA network or in any media format.
- will not enter, add, change, or delete Confidential Information to the UNISHKA network or any media format outside their scope of work.
- will not release or disclose UNISHKA Confidential Information other than what is required to perform their job-related duties and in accordance with applicable
- UNISHKA policies and procedures on releasing or disclosing Confidential Information.
- will not exhibit the contents of any Confidential Information on the UNISHKA network or in any media format to any person unless it is necessary to perform
- their job-related duties and in accordance with all applicable UNISHKA policies and procedures on exhibiting Confidential Information. (Refer to the policies mentioned above.)
- will keep personal passwords confidential and will not disclose them to anyone within or outside the organization. Passwords should be kept in
- secure places. Forgotten passwords and suspected compromises of passwords should be reported to the individual responsible for UNISHKA security or
- customer services and to the appropriate supervisor so the required action can be taken.
- will strive to keep Confidential Information on desktops or on computer screens from being viewed by others and will strive to ensure that computer
- screens are locked when away from their desk or office.
- will strive, for training purposes, to use simulated training information when possible; when this is not possible, will strive to protect and/or disguise

- any Confidential Information used for training purposes, including but not limited to, business system screen captures and business system instances.
- will strive to keep Confidential Information that is in any media format saved to their personal LAN drive and will strive to keep this information stored
- in a locked cabinet. Confidential information that requires viewing by more than one individual will either be stored on a restricted public drive or use
- a password protection feature.
- will strive to dispose of Confidential Information in accordance with applicable laws and/or UNISHKA policies on record retention.
- will not discard any Confidential Information in a waste receptacle or recycling bin (if applicable); will shred hard copy Confidential Information prior to disposal.
- will not remove Confidential Information from work premises without written authorization from the operations manager or designee.
- will not disclose Confidential Information to consultants without receiving prior approval from the operations manager or designee. In addition, consultants
- will not be allowed to remove Confidential Information from the premises without prior written approval from the operations manager or designee. Written
- approval indicates that a copy of the information can be removed from the premises but must be returned by a specified date.

Reporting a Suspected Violation(s)

UNISHKA employees and those acting on behalf of the UNISHKA must report a suspected violation(s) of this policy to the appropriate person (supervisor/manager, UNISHKA Director of Finance).

Disciplinary Action Regarding a Knowing Violation

For a UNISHKA employee, disciplinary action, up to and including termination, may occur if it is determined that a knowing violation(s) of this policy has occurred.

UNISHKA
Research Service