




**FORM FOR KEMPER CONTRACTORS AND CONTRACTORS' EMPLOYEES
WITH ACCESS TO KEMPER CORPORATION SYSTEMS**

Acknowledgement of Confidentiality and Security Obligations

In connection with the services ("Services") that I am performing as an independent contractor or an employee of a contractor for Kemper Corporation and/or its affiliates (collectively, "Kemper"), I acknowledge and agree to comply with the following:

1. I will maintain in confidence and take reasonable steps to protect the confidentiality of all information relating to the technical, financial, strategic, operational or other business affairs of Kemper, as well as its business partners, customers and other parties, as applicable, known by me, disclosed or otherwise made available to me in connection with the Services, including the subject matter of the Services and names of involved parties (collectively, "Confidential Information"). Confidential Information does not include information that is or becomes: (a) public knowledge through no fault of mine; or (b) known to me from a source not subject to any disclosure restrictions.
2. Except to the extent required in order to perform the Services in accordance with the agreement with Kemper, I will not: (a) use or disclose Confidential Information; (b) forward Kemper email to a personal or non-Kemper work email account; (c) save or download Confidential Information on non-Kemper equipment or systems; (d) download and install software on to Kemper computer equipment or systems without approval by Kemper Data Systems; (e) connect non-Kemper hardware devices to the Kemper network or any Kemper computing device; (f) conduct personal or other non-Kemper business on any Kemper computing device; or (g) use streaming technologies (e.g., internet TV, videos, music, etc.) through Kemper-provided internet services or systems.
3. I will return and/or destroy all Confidential Information in my possession or control at the conclusion of the Services, or at any time on request of Kemper.
4. I will promptly report known or suspected security issues to Kemper management, as described in Appendix A.
5. I have read and agree to comply with the statements outlined above, which reflect my personal responsibility as a user of Kemper resources, and to follow the best security practices outlined in Appendix B and the Code of Conduct and Ethics Principles for Business Partners attached as Appendix C.

Signature:	
Printed Name:	AYUB NADAF
Company Name:	CAPGEMINI - INDIA
Date:	02-July-2018

Note: This form must be signed and provided back to the Kemper assigned manager and is required as part of the contractor on-boarding process.



Appendix A – Examples of Information Security Incidents to be Reported Promptly

The following are examples of situations that may comprise or lead to a security incident. If you are a victim of, or become aware of, any of the following types of activities, report them promptly to your Supervisor, Corporate Security (KemperISIncidentResponse@kemper.com or 630.368.8029), and the local Help Desk. The list is not exhaustive.

B.1 Malicious Incident

- Computer infected by a virus or other malware (for example spyware or adware)
- Data altered by an unauthorized person.
- Receipt and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Response to a social engineering request - unknown people asking for information which could gain them access to the company's data (e.g. a password or details of a third party).
- Unauthorized disclosure of sensitive or confidential information electronically, in paper form or verbally.
- Deliberate damage or interruption to the organization's equipment or services.
- Unauthorized third party equipment connected to the company's network.
- Sharing confidential information to someone who shall not have access to it - verbally, in writing or electronically.

B.2 Access Violation

- Unauthorized access or use to the network, information repositories and secure premises.
- Intentional or inadvertent disclosure or exposure of log-in numbers or passwords.
- Inappropriate sharing of security devices such as access tokens.

B.3 Environmental

- Introduction of unauthorized or untested software.
- Information leakage due to software errors.

B.4 Inappropriate Use

- International access of inappropriate material on the internet.
- Use of unapproved or unlicensed software on the company's equipment.
- Misuse of company facilities or assets.

B.5 Theft / Loss Incident

- Theft / loss of files or data – whether hard copy or electronically held.
- Theft / loss of any of the company's equipment, e.g. computers, monitors, copiers, mobile phones, smart phones, memory sticks/thumb drives, CD/DVDs or access tokens.

B.6 Accidental Incident

- Inadvertent transmission of an email containing confidential information to unintended recipients or by "reply all".
- Receipt of unsolicited mail which requests the recipient to enter personal data.



Appendix B – Security Best Practices for Users

Do	Don't
Take responsibility for securing the information you create and manage.	Assume security is someone else's job and not your responsibility.
Report known or suspected security issues, such as a computer without antivirus software or a stranger calling and asking for inside information.	Fail to report security incidents for any reason, since without reporting, security issues cannot be resolved and future issues cannot be prevented.
Recognize sensitive information, such as medical, personnel, financial, trade secret, or confidential information, and ensure it is protected.	Share sensitive information with any unauthorized person, discuss it in public places, or store it in unsecured mobile devices.
Follow company policies by limiting your personal use of workplace resources and respecting copyright laws.	Use workplace resources to access inappropriate, sexually explicit, or threatening material.
Use secure forms of email or website portals when transferring sensitive information over the Internet.	Transmit medical, financial, trade secret, confidential, or other sensitive information over unencrypted channels.
Use a pass-phrase generated password that is strong and complex, e.g., "Welcome to the 1992 reunion." = "W2t1992r."	Write your password down on a piece of paper, or use easily guessed information, such as your birthday.
Inform the IT department if your computer lacks antivirus or antispyware software.	Download and install unapproved software from the Internet, which could contain malware or security holes.
Purchase and use mobile devices with security features such as password protection and encryption.	Place sensitive information on unsecured laptops, personal digital assistants, or smart phones.
Keep sensitive information locked away and inaccessible while you are away from your desk.	Forget to use a password protected screensaver to ensure no one accesses your computer while you are away from your desk.
Dispose of sensitive information properly, for example, by shredding paper documents with sensitive information.	Keep information indefinitely. Instead, follow our Records and Information Management Policy by securely disposing of information when its retention period expires.
Follow all laws, regulations, and policies, including our security policies, which apply to your job function and ask your supervisor when in doubt.	Bend or break security rules in order to "simplify" things. Instead, bring positive suggestions to your supervisor on how to securely increase efficiency.



Appendix C – Code of Business Conduct and Ethics Principles for Business Partners

10 Principles: principles that establish a framework and provide guidance to all employees and business partners on how to ensure ethical behavior while conducting business

Principle 1: We Avoid Conflicts of Interest

Principle 2: We Maintain Accurate Financial Books and Records

Principle 3: We Retain Records Properly

Principle 4: We Compete Fairly

Principle 5: We Strive to Comply with All Laws and Regulations

Principle 6: We Provide a Positive Work Environment

Principle 7: We Properly Use and Safeguard Company Assets

Principle 8: We Maintain the Confidences Entrusted to Us

Principle 9: We Want to Know When Something Is Wrong

Principle 10: We Are in This Together