SYNCORA HOLDINGS LTD.

CODE OF BUSINESS CONDUCT AND ETHICS

April 17, 2017

TABLE OF CONTENTS

Page

BUSINESS CONDUCT AND ETHICS

All references to "directors" shall include members of the Board of Directors of Syncora Holdings Ltd. or one of its subsidiaries, unless the context shall mean otherwise.

INTRODUCTION

Syncora Holdings Ltd. and all entities controlled by Syncora Holdings Ltd. (together with Syncora Holdings Ltd., "Syncora" or the "Company") have a strong commitment to the development of an organizational culture that encourages the highest standards of ethical conduct and compliance with all applicable laws. The Company strives to promote honest conduct and ethical business conduct by all Employees (as defined below) and compliance with the laws that govern the conduct of our businesses worldwide. We believe that a commitment to honesty, ethical conduct and integrity is a valuable asset that builds trust with our customers, suppliers, employees, shareholders and the communities in which we operate. To implement our commitment, we have developed this code of business conduct and ethics (the "Code"). Also, we have established a compliance program (the "Compliance Program") intended to ensure that we have in place policies and systems designed to prevent and detect violations. By design the Code goes beyond the requirements of applicable laws in certain respects. Our worldwide activities subject us to the laws of many jurisdictions. In some instances there may be differences between the laws of two or more countries. In that event, you must consult with the Compliance Director to understand how to reconcile any apparent conflict. This Code does not constitute a contract of employment, but has been designed to deter wrongdoing and to promote honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships and avoidance of conflicts of interest.

SCOPE

This Code applies to all controlled companies (as defined below) and all employees (including temporary employees), officers and directors of Syncora except where the application of certain requirements to non-management directors would be inappropriate (collectively, "Employee(s)"). In addition, anyone who acts on Syncora's behalf as a consultant or agent on a full-time or near full-time basis (i.e., regularly using Syncora's offices and having access to certain Company files, the IT network and other materials generally reserved for full-time employees) is expected to comply with the underlying principles of the Code when conducting business on behalf of the Company and the Company will distribute the Code to such consultants and agents as appropriate. For the purposes of the Code, a "controlled company" is one in which a Syncora company (or companies) owns an interest in excess of 50% or is otherwise designated as a controlled company by the Compliance Director. In addition to the Code, Senior Financial Officers are also subject to the Code of Ethics for Senior Financial Officers, attached hereto as **Appendix A**.

As to companies affiliated with Syncora but that do not fall within the definition of controlled company above, Company policy is to distribute the Code and Compliance Program to such affiliates and urge that they have in force similar polices and procedures to secure compliance with the principles of business integrity and ethics set forth in this Code.

COMPLIANCE PROGRAM RESOURCES

As part of our Compliance Program, we have appointed a Compliance Director and compliance attorneys and personnel whose names and telephone numbers are found at the back of this Code and are published on the shared (p://) drive in the Human Resources folder or will be provided to employees via email or other means. These resources are available to report violations and may be used to address questions concerning the Code and the Compliance Program. We encourage all Employees to ask questions regarding the application of the Code. Employees may direct such questions to their manager (in the absence of an actual or potential conflict of interest), a compliance attorney, or the Compliance Director. There are many types of ethical dilemmas that can arise in the working environment. The Code cannot address each and every situation, and so it is always recommended that Employees seek further guidance where required.

COMPLIANCE WITH LAWS, RULES AND REGULATIONS

It is the Company's policy to comply with all applicable laws, rules and regulations. Many of the Company's operating subsidiaries are subject to regulation in their territories of operation, the financial services industry being among the most highly regulated. The Code provides for compliance with the laws and regulations that apply to our business but does not cover regulatory compliance in detail. Regulatory compliance is overseen at a regulated entity level with each regulated entity having designated regulatory compliance staff and/or resources available to it.

Beyond the strictly legal aspects involved, Employees at all times are expected to act honestly and maintain the highest standards of ethics and business conduct, consistent with the professional image of the Company.

RESPONSIBILITIES

Employees individually are ultimately responsible for their compliance with the Code. Every manager will also be responsible for administering the Code as it applies to Employees and operations within each manager's area of supervision. Managers should coordinate these tasks with appropriate compliance personnel and may not delegate these responsibilities.

REPORTING

Employees who observe or become aware of a situation that they believe to be illegal, unethical or otherwise a violation of the Code, including situations which could implicate the Company in

unlawful conduct by others, have an obligation to notify their supervisor, manager, a compliance attorney, or the Compliance Director. Violations involving a manager should be reported directly to compliance personnel, not to or through the manager. When a manager receives a report of a violation, it will be the manager's responsibility to handle the matter in consultation with the Compliance Director. Matters relating to accounting or auditing or fraud within or against the Company should be reported directly to the Compliance Director or by calling the telephone numbers found at the back of this Code and/or otherwise provided to Employees. Any reports, calls or e-mails received will be treated fairly and respectfully. If an Employee would prefer to make a report via a telephone message and with no attribution, rather than speak to their supervisor etc., they can do so via a "compliance hot line" telephone number made available to all Employees[1].

If an Employee making a report wishes to remain anonymous, all reasonable steps will be taken to keep the employee's identity confidential, notwithstanding the fact that the report may have been made directly to the employee's supervisor, manager, a compliance attorney or the Compliance Director,. All communications will be taken seriously, and any reports of violations will be investigated.

Syncora will not tolerate retaliation for reports made in good faith and no adverse employment action will be taken against any employee making a good faith report. Any supervisor, manager or other Employee intimidating or imposing sanctions on an Employee will be disciplined, up to and including termination. If an allegation is made frivolously, in bad faith, maliciously, or for personal gain, disciplinary action may be taken against the person.

Employees should know that it is a crime to retaliate against a person, including with respect to their employment, for providing truthful information to a law enforcement officer relating to the possible commission of any federal offense. Employees who believe that they have been retaliated against by the Company, its Employees, contractors, subcontractors or agents, for providing information to or assisting in an investigation conducted by a federal agency, Congress or a person with supervisory authority over the Employee (or another Employee who has the authority to investigate or terminate misconduct) in connection with conduct that the Employee reasonably believes constitutes a violation of federal criminal fraud statutes or any rule or regulation of the Securities and Exchange Commission, may file a complaint with the Secretary of Labor, or in federal court if the Secretary does not take action in a timely manner.

In order to ensure that the conduct of all investigations conducted by the Company comply with applicable legal requirements, the Compliance Director, in consultation with the General

[1] Messages left on the "compliance hot line" are transcribed into a text which is e-mailed to the Compliance Director and the Company's General Counsel. An audio file of the message is retained which will be accessed if necessary to clarify the text transcription (i.e., if the text was not transcribed accurately and does not make sense on its face) or if the issue is deemed by the Compliance Director to be serious enough to warrant confirmation of the transcription.

Counsel or other appropriate legal counsel shall be consulted before the initiation of any investigation.

TRAINING

To ensure that all Employees understand their responsibilities under the Code, the Compliance Program includes training requirements. New Employees will receive introductory training on the principles of the Code as part of their orientation. All Employees will receive compliance training at least annually. All Employees whose functions or responsibilities involve compliance with the laws, regulations or standards of conduct applicable to our operations may receive additional specialized training, including participation in periodic training sessions as appropriate or required.

ACKNOWLEDGEMENT AND CERTIFICATION

The Code and the Compliance Program are available in printed form and also on (a) shared (p://) drive in the Human Resources folder; and (b) via email request from the Compliance Director or Human Resources Director. All Employees must read and understand the Code. On an annual basis, all employees and directors are required to complete an Acknowledgment form regarding compliance with the Code.

PROCEDURES REGARDING WAIVERS

Because of the importance of the matters covered by the Code, waivers will be granted only in limited circumstances and where circumstances would support a waiver. Waivers of the Code for Employees other than Executive Officers or Directors of Syncora may only be made by the Compliance Director, or the General Counsel who may act individually or together. Waivers of the Code, however, for Executive Officers or Directors of Syncora may only be made by the Board of Directors of Syncora or appropriate Board Committee and will be appropriately disclosed to Syncora shareholders in accordance with applicable law.

THE CODE OF BUSINESS CONDUCT AND ETHICS

A. AT-WILL EMPLOYMENT

The Company believes that its relationship with Employees will be mutually satisfying and beneficial. However, Employees should know there is no contractual right or obligation to remain in Syncora's employment or for Syncora to continue to employ Employees for any specified period of time. In the absence of a written agreement signed by an authorized officer of Syncora, all employment relationships with the Company are "at-will". This means that both the Employee and Syncora are able to terminate the employment relationship at any time for any reason or for no reason, and without providing prior notice. Additionally, the terms and

conditions of employment, including compensation, benefits and other privileges can be changed or eliminated without notice at any time, at the sole discretion of Syncora. It is important to note that NO persons other than the Office of the CEO of Syncora, or a designated individual authorized to act on its behalf can alter the "at-will" status of any employment relationship. Managers do not have the authority to enter into any type of contractual relationship with an Employee.

B. EMPLOYEE CONDUCT AND WORK RULES

Syncora's objective is to provide a positive work environment for all. To that end, Employees are expected to follow certain rules that benefit and protect the interests and safety of all other Employees and Syncora. Conduct that impairs the operation of the business, is contrary to the values that form the core of the Company, exposes Syncora to legal liability or financial loss, brings discredit to Syncora, or is offensive to customers or other Employees will not be tolerated and will subject you to disciplinary action up to and including termination of employment. The examples below, which are not all-inclusive, illustrate the types of behavior that are not permitted at Syncora:

- Insubordination, including improper conduct toward a manager, or refusal to perform tasks assigned by a manager in an appropriate manner including requests to work overtime.

- Refusal to follow Company policies and procedures.

- Harassing, sexually or otherwise, another employee, customer, supplier or independent contractor.

- The unauthorized use of alcoholic beverages while on Company premises, on Company time, on Company business, while operating Company-owned vehicles or equipment, or reporting for work while under the influence of alcohol.

- The unlawful possession, manufacture, sale, distribution, or use of a controlled substance, or reporting for work while under the influence of illegal drugs or narcotics.

- Theft, misuse, destruction or inappropriate removal or possession of Company property or of another individual's property, and the failure to report any knowledge of such acts.

- Falsifying any Company record or report, including time sheets.

- Possession of dangerous materials, such as explosives, firearms, chemicals or other similar items.

- Violence or threatening violence in the workplace.

- Unauthorized disclosure or use of business secrets or confidential information about Syncora or its customers.

- Failure to cooperate fully with and assist in an internal investigation pertaining to security, auditing, harassment, discrimination or work-related matters.

- Excessive lateness or excessive absenteeism, patterned absenteeism, or any absence without notice.

- Smoking in non-smoking areas.

- Unacceptable or unsatisfactory work performance or conduct.

- The recurrence of a problem that was the subject of prior corrective action.

- Violation of securities trading, insider trading and confidential information policies.

- Failure to report outside employment.

- Illegal duplication or acquisition of unauthorized copies of computer software.

- Inappropriate use of e-mail, voice mail, Internet, Intranet or other social media.

Again, these examples are illustrative. Although Syncora is an at-will employer, meaning that an Employee's employment has no specified term and may be terminated at any time by the Employee or Syncora with or without notice, Syncora may choose to exercise its discretion to utilize forms of discipline that are less severe than termination in certain cases. Syncora's use of less severe discipline will not change an Employee's at-will employment status.

C. ANTI-DISCRIMINATION/HARASSMENT

Syncora is committed to a work environment in which all individuals are treated with respect and dignity, one that promotes equal employment opportunities and that is free of discrimination, including harassment.

Sexual Harassment is discrimination and is illegal. Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature that are used as a term or condition of employment, or such conduct that has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment.

Sexual harassment may include a range of behaviors, depending on the circumstances, including, but not limited to:

- Requesting, explicitly or implicitly, submission to sexual demands as a term or condition of employment;

- Using sexual considerations as the basis for employment decisions such as promotions, salary increases, assigned duties, flexibility in hours, work force reduction, or any other condition of employment;

- Unwanted sexual advances or requests for sexual favors;

- Intimidating or hostile acts;

- Sexual jokes and innuendo;

- Verbal abuse of a sexual nature;

- Commentary about an individual's body, sexual prowess or sexual deficiencies;

- Leering, whistling or touching;

- Insulting or obscene comments or gestures;

- Display in the workplace of sexually suggestive objects, cartoons, pictures or other offensive materials;

- Using voicemail, e-mail or other technology and social media to communicate harassing messages; and/or

- Other physical, verbal or visual conduct of a sexual nature

Workplace harassment is defined as verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of his/her race, creed, color, sex, religion, national origin, age, sexual orientation, physical or mental disability, military or veteran status, citizenship status, marital status, ancestry, genetic information/characteristics or other characteristic protected by federal, state or local law and that has the purpose or effect of creating an intimidating, hostile or offensive work environment; unreasonably interferes with an individual's work performance; or otherwise adversely affects an individual's employment opportunities.

Workplace harassment may include, but is not limited to:

- Epithets, slurs or negative stereotyping;

- Threatening, bullying, intimidating or hostile acts;

- Denigrating jokes;

- Using voicemail, e-mail or other technology and social media to communicate harassing messages; and/or

- Written or graphic material that denigrates or shows hostility or aversion toward an individual or group;

Individuals and Conduct Covered

These policies concerning Sexual and Workplace Harassment apply to all Employees, whether related to the conduct of fellow Employees or all persons indirectly connected to Syncora, inclusive of interns, consultants, independent contractors and other service providers.

Conduct prohibited by these policies is unacceptable in the workplace or in any work-related setting outside the workplace such as during business trips, business meetings and business-related social events.

Reporting an Incident of Harassment, Discrimination or Retaliation

If any Employee, intern, consultant, independent contractor or other service provider feels that he or she has been the victim of discrimination, harassment or retaliation, or feels such an incident has taken place against another person, that individual should discuss his or her concerns immediately with a manager, or Human Resources in the event he or she is not comfortable discussing it with a manager. If an Employee would prefer to make a report via a telephone message with no attribution rather than to their manager etc., they can do so via a "compliance hot line" telephone number made available to all Employees (see Reporting section, page 3). See also the Complaint Procedure described in the next section.

In addition, we encourage individuals who believe they are being subjected to such conduct to advise the offender that his or her behavior is unwelcome and to request that it be discontinued. We recognize, however, that Employees may prefer to pursue the matter through the Company's Complaint Procedure.

Complaint Procedure

Any reported allegations of harassment, discrimination or retaliation will be investigated promptly by Human Resources. The investigation may include individual interviews with the parties involved, and, where necessary, with individuals who may have observed the alleged conduct or may have other relevant knowledge.

Confidentiality will be maintained throughout the investigatory process to the extent it is consistent with adequate investigation and appropriate corrective action.

Misconduct constituting harassment, discrimination or retaliation will be dealt with appropriately. Responsive action may include, for example, training, referral to counseling and/or disciplinary action such as warning, reprimand, withholding of a promotion or pay

increase, reassignment, temporary suspension without pay or termination, as Syncora believes appropriate under the circumstances.

Retaliation against an individual who reports harassment or discrimination, or who participates in an investigation of a claim of harassment or discrimination, is a serious violation of this policy and, like harassment or discrimination itself, will be subject to disciplinary action up to and including termination of employment. Acts of retaliation should be reported immediately and will be promptly investigated and addressed.

False and malicious complaints of harassment, discrimination or retaliation as opposed to complaints that, even if erroneous, are made in good faith, may be subject to appropriate disciplinary action. Additionally, any Employee of Syncora who fails to report violations of this Code or who fails to cooperate and facilitate an investigation may be subject to disciplinary action, up to and including termination of employment.

Conclusion

Syncora has instituted this policy to ensure a work environment that is free from harassment, discrimination and retaliation. The Company will make every reasonable effort to ensure that all concerned are familiar with these policies and are aware that any complaint under these policies will be investigated and resolved appropriately.

Employees with questions or concerns about these policies should speak with Human Resources.

D. SUBSTANCE ABUSE

Syncora is committed to a drug-free, healthful, safe and supportive workplace. Employees may not use, possess, distribute, sell, or be under the influence of alcohol or controlled substances. The legal use of prescribed drugs is permitted on the job only if it does not impair an employee's ability to perform the essential functions of his/her job both effectively and in a safe manner that does not endanger themselves or others in the workplace.

Violations of this policy will lead to corrective action, up to and including immediate termination of employment, and/or required participation in a substance abuse rehabilitation or treatment program. Such violations may also have legal consequences.

Syncora provides access to an Employee Assistance Program, a confidential service that offers qualified alcohol or drug rehabilitation counseling. You are encouraged to seek assistance before drug or alcohol usage results in work performance problems or disciplinary action. Your request for assistance will be kept confidential. For more information on the EAP, consult the benefits plans on the shared (p://) drive in the Human Resources folder.

Alcohol at Company Functions

Syncora recognizes that in some business situations serving alcohol is customary. In these situations, you should not consume alcohol in excess and you should be sure your drinking does

not lead to a safety hazard for yourself, other Employees or the public. Syncora managers who attend functions where alcohol is being served are accountable for ensuring this policy is followed. The Company will pay for alternate transportation home for any Employee or guest who the Company feels is not capable of operating a motor vehicle.

Drug Free Workplace Act
Syncora complies with specific provisions of the Drug-free Workplace Act. If you are directly involved with federal government contracts and are convicted of any criminal drug offense occurring in the workplace, you must notify Human Resources within five days of the conviction. Syncora will take appropriate action, including notifying the federal contracting officer of the conviction within 10 days.

E. USE OF COMPANY PROPERTY

All Company facilities, equipment, supplies and bulletin boards are to be used for Company-related business only. Subject to Sections F and G below, the use of Company equipment (for example telephones, voice-mail, computers, Blackberries) is also limited to Company-related business, except for occasional personal purposes. Excessive use of these devices for non-work purposes may result in disciplinary action up to and including termination of employment.

Employees' use of Company property is subject to monitoring to the extent allowed by law.

F. INFORMATION TECHNOLOGY

The use of technology resources -- including, without limitation, computers, Blackberries, e-mail, voice mail, Internet access and electronic social media -- to facilitate the effective communication of business-related data has become essential to the way we do business. Although these resources promise faster and better communications, they also raise significant issues concerning the accuracy, security and control of information. This policy serves to define the parameters of appropriate and professional use of Company technology resources.

This policy applies to (1) all Employees and all other persons authorized to use Company technology resources (collectively, users); (2) all Company-provided technology resources, including, but not limited to, computers (e.g., desktop and portable computers, servers, networks, printers, software, telephones, Blackberries and data storage media), e-mail, voice mail, text messaging, and Internet use (collectively, technology resources); and (3) all data or communications created, entered, received, stored, viewed or transmitted by the use of Company technology resources, including, but not limited to, all non-public information (e.g., information about the Company's operations, methods, processes, research and development, personnel, employee medical files, owners, finances, costs, profits, customers and plans) that belongs to the Company and disclosure could harm the Company and/or its employees and provide an unfair advantage to the Company's competitors.

Other than occasional non-work related use of e-mail and Internet access, Company technology resources may be used only for legitimate business-related communications. Occasional non-work related use means infrequent, incidental use that is professional, in good taste and does not interfere with Company business, the performance of the user's duties or the availability of technology resources. All use of Company technology resources -- including all non-work related use -- is subject to this policy. Users are encouraged not to use Company technology resources for non-work related purposes, and to confine such activities to personal email accounts and equipment.

Users have no expectation of privacy in connection with the use of Company technology resources, including the creation, entry, receipt, storage, viewing or transmission of data.

As with all other Company property, Company technology resources and all data created, entered, received, stored, viewed or transmitted via those resources are subject to search, monitoring, inspection, review, access and disclosure for any reason, at any time, and without advance notice by persons designated by or acting at the direction of the Company's President, Information Technology Manager, and/or Human Resources Manager, or as may be required by law or as necessary for, or incidental to, auditing, security and investigative activities, and to ensure effective technology resource administration and policy compliance. For example, authorized persons may inspect the Company's technology resources to investigate theft, the disclosure of proprietary information, misuse, and to assess productivity and Internet use. As to the latter point, the Company monitors web sites visited and blocks access to offensive sites. All activity (i.e., sites visited) may be logged. The Information Technology Department will compile such data, which will be available for review by management and/or its designee.

Users must understand that their use of passwords will not preclude access, monitoring, inspection, review, or disclosure by authorized Company personnel. The Company also may unilaterally assign and/or change passwords and personal codes.

The security of the Company's computer system is every user's responsibility. In this regard, no matter how much technology is dedicated to making the system secure, security cannot be ensured without the cooperation and vigilance of every user. Passwords may not be shared with anyone — sensitive data is at stake. It is best practice for passwords not to be dictionary words or names of people or pets. The best passwords are random sequences of letters and numbers.

Unauthorized access of e-mail, data, and use and/or disclosure of other users' passwords is strictly prohibited. For example, unauthorized use of other user's passwords is prohibited, as is accessing other users' files or communications without any business purpose, e.g., to satisfy idle curiosity.

All electronic communication systems are provided for business use. It is your responsibility to read and understand all policies related to Information Technology. Please refer to **Appendix D** for the Company's Information Risk Management Policy.

All Employees and all other persons who use Company technology resources must sign the attached Acknowledgment and Statement of Agreement. The Human Resources Department will retain the Acknowledgments in users' personnel files.

G. ELECTRONIC SOCIAL MEDIA ACTIVITY POLICY

This policy applies to writing, posting or otherwise contributing to: blogs or microblogs (such as Twitter), personal websites or webpages; listservs or mailing lists; social networking or other similar sites (such as Facebook, MySpace, and LinkedIn); audio, photo or video sharing websites (such as YouTube, Google Video, Flickr and Picasa); virtual worlds (such as Second Life); or other user-generated electronic media. Employees of the Company should not have any expectation of privacy with regard to their use of Company-provided equipment, systems or software.

The Company recognizes that participating in electronic social media is often a personal activity, but seeks to regulate such activity when it impacts the Company, Company Employees or third parties who deal with the Company. Employees using the internet to actively visit websites containing pornographic materials are subject to termination.

With regard to their activities both outside of work and during working hours, Employees should remember that information placed on any electronic medium, and data sent via other electronic methods (e.g., email and text messages) can easily become public. Specifically, other Employees, potential Employees, vendors, and customers of the Company and third parties may use electronic media and search engines to obtain information from the content that Employees post, including information about the Company and its activities. Given this reality, all Employees must consider the impression they create about themselves and the Company when they place information concerning or identifying the Company, its Employees or its activities on any electronic medium. The Company trusts that its Employees will act responsibly, exercise good judgment and the highest degree of professionalism and respect confidentiality when communicating any information that concerns or identifies the Company or any of its Employees. If an Employee fails to act responsibly in that regard, the information that he or she communicates may cause harm to the Company, its Employees, or others.

Therefore, if Employees choose to engage in electronic media activity, even when not working, on their own time and using their own equipment and systems, Employees should observe the following guidelines:

- First, Employees engaged in personal electronic media activity that is not related to their job responsibilities, including, but not limited to, blogging, social networking, or instant messaging, should do so using a personal account. Company-provided e-mail, Internet or IM accounts, that identify an Employee as a Company employee, should not be used either to access such services or to identify an Employee on such social networks.

- Second, Employees discussing the Company or their position at the Company online, must take care to follow this Code, including, but not limited to, its policies against

workplace harassment, discrimination and retaliation. Employees should not discuss the Company, its management, or their supervisors or co-workers in a manner that could defame any individual or damage any person's reputation. Social media activity that violates any Company policy may result in discipline up to and including termination of employment.

- Third, Employees' blogs, messages, comments or posts relating in any way to the Company, or to their job, should contain a disclaimer clearly stating that they are expressing only their personal opinions that have not been reviewed by, are not endorsed by and do not represent the opinion or viewpoints of the Company. Similarly, Employees discussing the Company's products or services online, should disclose their affiliation with the Company, and include a disclaimer communicating that you are speaking only for yourself and not for the Company. Employees asked to provide information about the Company while participating in electronic discussions, should direct such inquiries to Human Resources.

- Fourth, Employees may not disclose any documents or information concerning the Company, its Employees or others that could be considered proprietary, confidential, or intellectual property, and may not use the Company's logo, graphics, trademarks, trade names, or corporate slogans. Again, remember that messages, blogs and other electronic media may be public and accessible to third parties, including the Company's competitors, vendors and customers. Thus, it is critical that Employees maintain the confidentiality of non-public Company information and abide by the terms of any confidentiality agreement that you have signed.

- Fifth, Employees should not discuss the Company's customers, suppliers or vendors without their explicit prior approval. Employees should work through their supervisor to obtain such prior approval, when necessary.

- Sixth, Employees should respect all copyright laws. As a general rule, Employees should not distribute or incorporate material retrieved or copied from another web site or publication, unless the usage of such material meets the legal definition of "fair use." An Employee who wishes to reproduce the contents of an electronic or print publication for job-related purposes should contact the Legal Department to determine whether such use is proper.

- Seventh, while online, Employees should follow all applicable financial disclosure or securities laws and regulations, as well as any agreements with the Company.

Please remember that the Company may monitor blogs, social networking sites or other electronic media. Employees who fail to abide by these guidelines or the Company's Code of Conduct or policies while online, may be subject to legal or disciplinary action by the Company and/or others. Employees should contact the Human Resources Department with any questions or concerns about any aspect of this policy.

H. REPORTING OF UNETHICAL BEHAVIOR AND POLICY AGAINST RETALIATION

Employees who observe or become aware of a situation that they believe to be a violation of the Code, have an obligation to notify their manager, Human Resources, a compliance attorney, or the Compliance Director, unless the Code directs otherwise or provides an alternative complaint procedure (see Section C). When a manager receives a report of a violation, it will be the manager's responsibility to handle the matter in consultation with the regional compliance officer. Violations involving a manager, however, should be reported directly to Human Resources or compliance personnel, not to or through the manager. All communications will be taken seriously and any reports of violations will be investigated.

I. HONEST AND FAIR DEALING, CONFLICT OF INTEREST, CORPORATE OPPORTUNITY AND PROTECTION AND PROPER USE OF COMPANY ASSETS

Employees must endeavor to deal honestly, ethically and fairly with the Company's customers, suppliers, competitors and other employees. No employee should take unfair advantage of anyone through manipulation, concealment, abuse of confidential or privileged information, misrepresentation of material facts, or any other unfair-dealing practice.

Unfair dealing is not only unethical but, in some circumstances, such conduct may give rise to allegations of fraud and thereby expose Employees and the Company to criminal and/or civil liability for an alleged violation of anti-fraud laws or possibly, antitrust laws. Conduct which involves the use of deception, which would include a knowing misrepresentation omission concealment of a material fact, designed to induce another to act to his or her detriment, constitutes fraud and could result in criminal charges, civil liability and/or disciplinary action.

The scope of actionable fraud goes beyond the Company's transactions with clients and includes making false entries in the Company's books and records, producing false financial statements as well as the circumvention of the Company's internal controls. In addition, the Company may be the victim of fraud perpetrated by others, such as Employees who may misappropriate Company assets or falsify expense reports, and vendors who may overcharge, duplicate invoice or issue fictitious invoices, as well as agents who may misreport premiums or falsify claims.

Employees who suspect or know of fraudulent activity involving the Company, including efforts by persons outside the Company to defraud the Company, have an obligation to promptly report such information, following the procedures set forth in the Reporting section of this Code (see section on Reporting, page 3).

Employees must a) avoid any interest that conflicts or appears to conflict with the interests of the Company or that could reasonably be determined to harm the Company's reputation and b) report any actual or potential conflict of interest (including any material transaction or relationship that reasonably could be expected to give rise to such conflict) immediately to the

Compliance Director and adhere to instructions concerning how to address such conflict of interest. A conflict of interest exists if actions by any Employee are, or could reasonably appear to be, influenced directly or indirectly by personal considerations, duties owed to or acts performed for persons or entities other than the Company, or by actual or potential personal benefit or gain. Employees may not become a director, officer, employee, agent or advisor to any company outside the Company without the prior written approval of the Compliance Director unless the service complies with the Policy on Syncora Directors serving on the Boards of Syncora affiliated companies. Related Party transactions, that is, transactions between any Syncora company and an Employee (or a company in which any such Employee has an interest, excluding modest ownership interests in publicly traded companies) requires the approval of the Compliance Director. Certain transactions between a Syncora company and a Syncora Executive Officer or Director may require the approval of an appropriate committee of the Board of Directors.

In addition, Employees owe a duty to advance the legitimate interests of the Company when the opportunities to do so arise. Employees should not, when advancing the legitimate interests of the Company, use these opportunities to further their own personal interests. Employees must also protect the Company's assets, not use such assets for personal profit and ensure such assets efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability. All Company assets should be used only for legitimate business purposes.

Providing loans to, or guarantees of obligations of, Employees or their family members will not be allowed without the prior written approval of the General Counsel, and if appropriate, the Board of Directors or a committee of the Board. The Company will not extend, maintain or arrange for any personal loan to or for any director or executive officer (or the equivalent thereof).

By way of example, conflicts of interest can include:

1. ownership by an Employee or family member of a significant financial interest in an entity which does or seeks to do business with, or is a competitor of, Syncora;

2. serving as a director, officer, partner, consultant or other key role with an entity which does or seeks to do business with, or is an actual or potential competitor of, Syncora;

3. ownership of or employment with another business entity that would interfere with an Employee's ability or desire to perform properly his or her duties to Syncora;

4. acceptance of gifts or gratuities by an Employee or family member the nature of which exceeds common courtesies extended in accepted business practice or which raise any implication that could be construed as affecting the Employee's judgment or decision making;

5. situations in which an Employee, or an Employee's family member receives improper personal benefits as a result of his or her position in the Company; and

6. any outside activity that might reasonably be expected to affect adversely Syncora's interests.

Related party transactions, that is, transactions between any Syncora company and an Employee or a company in which any such Employee has an interest excluding modest interests in publicly traded companies) requires the approval of the Compliance Director. Certain transactions between a Syncora company and a Syncora Executive Officer or Director may require the approval of a committee of the Board of Directors where appropriate. (see **Appendix B**, Procedures for Approval of Related Party Transactions.)

Full-time Employees have a primary, professional obligation to the Company and to its shareholders. Therefore, all such Employees should keep any outside activity (including self-employment) totally separate from employment with the Company. Full-time Employees are expected to devote the use of the Company's time working on behalf of the Company. Unless expressly authorized by the Compliance Director, no outside activities should involve the use of the Company's time, name, influence, assets, funds, materials, facilities or Employees. Any appointment of an Employee to a governmental commission, service organization or professional body that would involve designating the Employee as representative of the Company requires pre-approval of the Compliance Director. Employees may not become a director, officer, employee, agent or advisor to any company outside the Company without the prior written approval of the Compliance Director unless the service complies with the policy on Syncora Directors serving on the Boards of Syncora Affiliated Companies (See **Appendix C** attached hereto).

In addition, Employees owe a duty to advance the legitimate interests of the Company when the opportunities to do so arise. Employees may not personally take for themselves opportunities that are discovered through the use of corporate property, information or position. Employees must also protect the Company's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability. All Company assets should be used only for legitimate business purposes.

J. CONFIDENTIALITY

Employees may have access to proprietary and confidential information concerning the Company's business, clients and suppliers. Employees are required to keep such information confidential during employment as well as thereafter, and not to use, disclose, or communicate that confidential information other than in the course of employment. The consequences to the Company can be severe where there is unauthorized disclosure of information pertaining to internal matters or developments, or by the unauthorized disclosure of any non-public, privileged or proprietary information. In addition to possibly violating the law, such disclosure could, among other things, competitively disadvantage the Company or breach the confidence of a client of the Company. No current or former Employee may disclose any attorney-client

privileged information or any attorney work product without the prior written consent of the General Counsel. Proprietary or confidential information obtained by Employees in other capacities (including former employment) should not be used in violation of any applicable restrictions on the use of such information. Employees should inform their supervisors if they are subject to any such restrictions. Finally, the theft or knowing receipt of stolen proprietary information is a crime in most jurisdictions. Should you be offered or discover another's proprietary information, or become aware of the existence of misappropriated information you should immediately contact a compliance attorney.

The use of the term "confidential information" includes information not generally known outside the Company in whatever form regarding the business, accounts, finances, trading, planning, software, or know-how of the Company, its insureds, reinsureds and other existing or prospective customers or clients. It also includes such information designated by the Company as confidential or information that an Employee is aware is subject to an obligation of confidentiality. Company records, reports, data, software, electronic files, data bases, and documents are confidential and you are not permitted to disclose or release them to persons who are not Employees of the Company, remove them or make copies of them, in whole or in part, without prior approval of the owner of the information and/or your manager. Employees must take due care to ensure that confidential data in electronic format is protected in transmission and storage by using Company-supplied secure email and encryption mechanisms. Except as required in the performance of employment duties, or by law after consulting with the Compliance Director should not discuss business transactions or Company business with anyone who does not work for Syncora or with another Company Employee who does not have a direct association with the transaction. Furthermore, you should refrain from discussing confidential information while in any non-private setting.

If you are questioned by someone outside your department and you are concerned about the appropriateness of giving them information, you are not required to answer. Instead, refer the inquiry to your manager and reference the Company's Confidentiality policy. Any inquiries from someone outside the Company concerning the Company's business should be referred to the Company's Compliance Director or the Legal Department[2].

In addition, Employees owe a continuing obligation of confidentiality after leaving the Company's employment. Employees may not disclose the Company's confidential information to any third party after leaving employment except with the prior written consent of the Company or as required by applicable law.

Upon termination of employment, Employees may be asked to sign a declaration confirming their continued obligation of confidentiality owed to the Company and confirming they have returned all Company property.

---

[2] Inquiries from shareholders of the company or representatives of the media should be referred to the Chief Administrative Officer (see also Section K below).

In addition to protecting our own proprietary information, it is the policy of the Company to respect the proprietary information of others. In many jurisdictions, the theft or knowing receipt of stolen proprietary information is a crime. Should any Employee be furnished with someone else's proprietary information or become aware of information that they believe may have been misappropriated from another party, that Employee should immediately report the event to the Compliance Director.

No current or former Employee shall disclose any attorney-client privileged information or any attorney work product without the prior written consent of the General Counsel. Any violation of the Policy on Confidentiality will be grounds for disciplinary action, up to and including termination, in addition to any other remedies available at law.

K. CORPORATE COMMUNICATIONS

Media: Employees should send any and all direct press enquiries, including requests for information, interviews or editorial contributions, to the Chief Administrative Officer and the Legal Department. Furthermore, all media relations activities must also be approved in advance by the Chief Administrative Officer and the Legal Department. Employees exposed to media contact when in the course of employment must not comment on rumors or speculation regarding the Company's activities.

Press Releases: The Chief Administrative Officer and the Legal Department must be notified of all press releases before they are issued. The Chief Administrative Officer and the Legal Department are jointly responsible for vetting and approving all releases issued by Syncora or any of its companies.

Conferences: Employees who are asked to address external meetings or conferences on behalf of the Company must notify the Chief Administrative Officer, the Compliance Director and the Legal Department and obtain prior approval of speeches and/or presentations. In the case of investor conferences, Investor Relations Department should be notified and provide approval of speeches and/or presentations.

Endorsements: The use of Syncora's name by non-Syncora entities is generally discouraged. However, all requests for Syncora or its Employees to allow Syncora's name to be used to endorse products, services, companies, programs etc. must be submitted to the Chief Administrative Officer, the Compliance Director and the Legal Department, accompanied by a business rationale as to why the request should be approved. The request will then be reviewed jointly by the Chief Administrative Officer, the Compliance Director and the Legal Department.

Regulatory Inquiries: All inquiries from regulatory authorities or government representatives should be referred to the Compliance Director and the General Counsel.

Regulation FD: In addition, senior management, investor relations professionals and others at Syncora who regularly communicate with securities market professionals ("FD Person(s)") and with holders of Syncora securities are encouraged to comply with the Regulation on Fair

Disclosure promulgated by the Securities and Exchange Commission the ("SEC") ("Regulation FD"). Regulation FD provides that whenever any FD Person discloses material, non-public information to certain persons (generally, securities market professionals and holders of Syncora securities who may trade on the basis of such information), Syncora may disclose that information to the general public either simultaneously (for intentional disclosures) or promptly (for inadvertent disclosures).

L. SECURITIES TRADING

Syncora Holdings Ltd. is a public company listed on the pink sheets and, accordingly, is subject to stringent rules relating to transactions in its securities.

Employees, their family members others living in the same household, friends, acquaintances, the media, or analysts (collectively, "tippees") are prohibited from trading securities while in possession of material, non-public information relating to the Company or any other company, including a customer or supplier that has a significant relationship with the Company. Information is "material" when there is a substantial likelihood that a reasonable investor would consider the information important in deciding whether to buy, hold or sell securities. In short, any information that could reasonably affect the price of securities is material.

Information is considered to be "public" only when it has been released to the public through appropriate channels and enough time has elapsed to permit the investment market to absorb and evaluate the information.

Material, non-public information should only be disclosed to key personnel and outside advisers whose work for the Company requires that they have such information. All persons given access to such information should be advised of their insider status and, if necessary, be required to sign a confidentiality agreement or told not to disclose the information further except as absolutely necessary for corporate purposes. Such information must not be passed on to others, including family members and other tippees.

In order to protect the Company and its Employees from liability that could result from a violation of legal requirements, the Company requires Employees to engage in purchases or sales of Syncora securities only during "Window Periods". Currently, Window Periods begin each quarter at the opening of trading on the third full trading day following the later to be publicly released of the Company's stautory or GAAP financial results (the "Open Window Date") and end on the tenth full business day following the Open Window Date. At the Company's discretion, trading outside a Window Period may be permitted on a case-by-case basis with the prior approval of the Compliance Director. No person may buy or sell Syncora securities, even during Window Periods, if such person is in possession of material, non-public information. If an Employee leaves his or her employment during a Closed Window Period (or blackout period) the former employee must abide by Syncora's securities trading policy until the next open Window Period or obtain an exception from the Compliance Director.

At any time, the Compliance Director with consultation of appropriate legal counsel has authority to designate a "blackout period" over all trading in Syncora securities (even during a Window Period). A blackout period compels all trading in the securities affected to cease immediately for the period designated by the Compliance Director. A blackout period may be exercised over securities of companies with which the Company does or may do business or in which the Company invests or may invest. No one may disclose to any outside third party that a blackout period has been designated.

From time to time, the Company may grant Employees options to purchase Syncora securities at a certain price for a certain period of time. The Company has no obligation to monitor the status of such options including informing Employees when options are due to expire. Accordingly, in no event should an Employee rely on the Company to monitor the status of any such award and the Company will not be responsible for decisions that employees make regarding the exercise of such options.

With the prior specific written approval of the Compliance Director as to the particular plan or arrangement, officers and directors of Syncora may establish appropriate plans or arrangements that meet the "safe-harbor" provisions of Rule 10b5-1. That safe-harbor provides that a purchase or sale under such a pre-approved plan or arrangement is not on the basis of "material non-public information" if certain conditions specified in that Rule are satisfied. (However, the establishment of any such plan or arrangement is subject to the requirements of the policy on pre-clearance, window periods and blackout periods).

Failure to comply with the Company's securities trading policy may subject Employees or Employees' family members to criminal or civil penalties, as well as to disciplinary action by the Company up to and including termination for cause. Responsibility for complying with applicable laws as well as the Company's policy rests with Employees individually.

Please direct all inquiries concerning the Company's securities trading policy or the application of U.S. or other applicable insider trading and tipping laws to the Compliance Director, General Counsel or other internal legal counsel.

Pre-clearance of Trades by Employees Designated as Restricted Group Members

To prevent inadvertent violations and avoid even the appearance of an improper transaction (which could result, for example, where an Employee engages in a trade while unaware of a pending major development), the procedure set forth below must be followed by those Syncora Employees designated from time to time by the Compliance Director as restricted ("restricted group members").

Any transactions in Securities of Syncora or other companies with which Syncora does or may do business or in which Syncora invests or may invest ("Other Companies") by any restricted group member (which includes executive officers and directors of Syncora must be cleared in advance by the Compliance Director. Directors may trade in securities of Other Companies

without prior approval of the Compliance Director if they are unaware that the company is an Other Company or if they are not in possession of inside information with respect to the Other Company.

Transactions in Syncora securities by the persons listed below should be pre-cleared because such transactions may be attributed to a restricted group member:

- any member of a restricted group member's household;
- any trust or estate in which a restricted group member or a household member is a settlor, beneficiary, trustee, executor or the like;
- any partnership in which a restricted group member or a household member is a general partner;
- any corporation in which a restricted group member or any household members either singly or together own a controlling interest or otherwise control the corporation; or
- any trust, corporation, charitable organization or other firm, entity or group where a restricted group member or a household member has or shares with others the power to decide whether to buy or sell Syncora securities.

If, upon requesting approval, a restricted group member is notified that he / she may make the specified trade, then such transaction must take place within 14 days of the date of such approval (subject to the other restrictions imposed by this policy) or such shorter period as the Compliance Director may designate. If, for any reason, the trade is not completed within such period, clearance must be obtained again before the proposed trade may occur.

If, upon requesting approval or otherwise, a restricted group member is advised that the proposed trade may not occur, that restricted group member may not, under any circumstances, buy or sell any Syncora securities or any securities of an Other Company nor may such restricted group member inform anyone of the restriction. This trading restriction will apply until the restricted group member receives subsequent written clearance to trade.

The buying and selling of Syncora shares, or the selling and buying of Syncora shares, by a director or executive officer of Syncora[2] within any period of less than six (6) months requires disgorgement of "profits"[3], except in certain limited circumstances.

---

[2] For U.S. Securities Exchange Act Section 16 purposes, "officer" is defined to mean "an issuer's president, principal financial officer, principal accounting officer (or, if there is no such accounting officer, the controller), any vice-president of the issuer in charge of a principal business unit, division or function (such as sales, administration or finance), any other officer who performs a policy-making function, or any other person who performs similar policy-making functions for the issuer. Officers of the issuer's parent(s) or subsidiaries shall be deemed officers of the issuer if they perform such policy-making functions for the issuer."

The Compliance Director will identify those persons who should consider themselves officers for these purposes.

No Trading in Derivatives

Employees shall not engage, at any time, in the following activities with respect to Syncora securities:

1. Short sales;

2. Purchases on margin or using Syncora securities as margin collateral;

3. Buying or selling put options or call options;

4. Using Syncora shares as collateral for a loan or other obligations if the applicable terms allow for the immediate sale of those shares or during a closed window or trading blackout period; or

5. Enter into hedging transactions (e.g., credit default swaps) for the purpose of purchasing credit protection on Syncora securities.

Transactions described in items 2 and 4 above may be conducted with the prior written consent of the Compliance Director.

M. INTEGRITY OF RECORDS, ACCOUNTING PROCEDURES AND FRAUD PREVENTION

Accuracy, reliability and timeliness in the preparation of all financial and business records is mandated by law and is of critical importance to the Company's decision making process and to the proper discharge of Syncora's financial, legal and reporting obligations. The books, records and disclosure provisions of the U.S. Federal Securities Laws, the U.S. Foreign Corrupt Practices Act and other applicable laws require companies to maintain accurate books and records and to devise, and have in place, an adequate system of internal controls. Such laws may provide for criminal and civil penalties for violations of these requirements. The books and records provisions of the Foreign Corrupt Practices Act require that where the Company holds 50% or less of the voting power with respect to a domestic or foreign firm, the Company must proceed in good faith to use its influence, to the extent reasonable under the circumstances (such as degree of ownership and laws and practices governing the business operations of the country where the firm is located), to cause the domestic or foreign firm to devise internal controls

---

Footnote continued from previous page.

[3] "Profits" are computed under the "lowest-in, highest-out" method, by matching the highest sale price with the lowest purchase price within six months, the next highest sale price with the next lowest purchase price within six months, and so on, with no netting of losses against profits.

consistent with the specific books and records and internal accounting controls spelled out in the statute.

All business records, expense accounts, vouchers, bills, payrolls, service records, reports to government agencies and other reports must accurately reflect the facts. Without limiting the foregoing, all reports and documents filed with the SEC, as well as other public communications should be full, fair, accurate and understandable.

All corporate funds and assets must be recorded in accordance with Company procedures. The books and records of Syncora must be prepared with care and honesty and must accurately reflect each transaction recorded therein. False or misleading entries in such records are unlawful and are not permitted. No undisclosed or unrecorded funds or assets shall be established for any purpose. Where the Company permits petty cash funds to exist, such funds must be administered pursuant to the Company's system of internal controls. Except for petty cash approved by the relevant business unit controller, no cash funds may be maintained. Electronic transfers of funds are not considered cash transactions but must be conducted in accordance with Company policy. The use of Company assets for any unlawful or improper purpose is strictly prohibited.

Employees must not, and must not direct others to, take any action to fraudulently influence, coerce, manipulate or mislead any public or certified public accountant engaged in the audit or review of the Company's financial statements for the purpose of rendering those financial statements materially misleading; nor may they take any such action at the direction of any Employee. Examples of actions that could result in rendering financial statements materially misleading include: issuance of a report on the Company's financial statements that is not warranted in the circumstances due to material violations of generally accepted accounting principles, generally accepted auditing standards, or other standards; non-performance of audit, review or other procedures required by generally accepted auditing standards or other professional standards; failure to withdraw an issued report under appropriate circumstances; and failure to communicate matters to the Company's Audit Committee. Any such actions could be deemed by regulation, law or the Company to be "for the purpose of" rendering the financial statement misleading if the person involved knew or was unreasonable in not knowing that the improper action, if successful, would result in rendering financial statements materially misleading. Syncora is firmly committed to the prevention and detection of fraud. Fraud could have a material impact on the integrity of our financial statements and on our reputation.

To this end, Syncora has:

- introduced appropriate measures to minimize the risk of fraud;
- provided appropriate mechanisms for employees to report instances of fraud, or potential fraud, while remaining anonymous, if they desire; and
- adopted procedures to investigate suspected fraud.

Unlike error, fraud is intentional and usually involves deliberate concealment of the facts with the intent to deceive. It may involve one or more members of management, employees, or third parties. Fraud could potentially give rise to misstatement of our financial statements, including:

- misstatements arising from fraudulent financial reporting (such as improper revenue recognition, overstatement of assets or understatement of liabilities);
- misstatements arising from misappropriation of assets (wire fraud, fictitious vendors);
- expenditures and liabilities for improper purposes;
- fraudulently obtained revenue and assets, or the avoidance of costs and expenses; and
- fraud in our fulfillment of disclosure obligations.

Syncora has created accounting controls intended to mitigate the risk of fraud. Fraud is also specifically considered through a risk and control assessment process involving the Finance Department. Controls that mitigate the risk of fraud are reviewed. Employees are encouraged to bring to the attention of their manager or the Compliance Director any opportunities or motives for fraud they do not think are adequately covered by the Company's existing controls (see section on Reporting, page 3). These controls include segregation of duties, proper review and authorization procedures, and independent monitoring of data and documentation.

N. ENTERTAINMENT GIFTS AND PAYMENTS

Syncora will procure and provide goods and services based on service and quality. Decisions by the Company relating to the procurement and provision of goods and services should always be free from even a perception that favorable treatment was sought, received or given as the result of furnishing or receiving gifts, favors, hospitality, entertainment or other similar gratuity. The giving or receiving of anything of value to induce such decisions is prohibited.

Providing or receiving gifts or entertainment of nominal value motivated by commonly accepted business courtesies is permissible, but not if such gifts or entertainment would reasonably be expected to cause favoritism or a sense of obligation.

The payment of Syncora funds to any officer, Employee or representative of any customer or supplier in order to obtain any benefit, such as to induce the purchase or sale of insurance and reinsurance and other goods or services, is strictly prohibited. The competitive appeal of the Company's services and products must be based on their quality, price and other legitimate attributes recognized in the marketplace.

Syncora Employees shall not seek or accept any personal gifts, or any allocations of shares in an initial public offering, payments, fees, services, valuable privileges, vacations, loans or pleasure trips without a business purpose from any person or business organization that does or seeks to do business with, or is a competitor of, the Company. No Employee shall accept anything of value in exchange for referring business opportunities to another business.

Gifts or entertainment of reasonable value motivated by commonly accepted business courtesies may be offered or accepted, but not if such gifts or entertainment would reasonably be expected to cause favoritism or a sense of obligation to the donor. Spousal travel (which is intended to be reimbursed by the Company or by a customer or supplier) must be pre-approved by senior Business Unit or segment management. Meals or entertainment provided by or to an existing or potential customer or supplier must be reasonable, for a business purpose, and not occur on a repetitive basis. Meals or entertainment may not be supplied to a customer if it would violate a known customer policy. If an unsolicited gift of more than nominal value is received, the Employee should return the gift with a polite note explaining Syncora's policy.

It is difficult to promulgate a rule as to what is "nominal" or "reasonable" or what is a "commonly accepted business courtesy" to cover all circumstances. Employees are therefore urged to make good faith judgments and to ask themselves whether it would be embarrassing to him or her or the Company if a story appeared in the local newspaper about the giving or receiving of the gift or entertainment in question. In cases of doubt, you must seek guidance from the Compliance Director.

Syncora's business entertainment must not be conducted at any location that could adversely affect Syncora's reputation.

Gifts to and entertainment of government officials of the U.S. and other jurisdictions, are subject to very strict restrictions and must be pre-approved by the Compliance Director.

O. POLITICAL CONTRIBUTIONS

Certain jurisdictions have enacted laws prohibiting contributions (directly or indirectly) by corporations to political parties or candidates. For example, U.S. federal law prohibits such contributions in connection with federal elections, primaries or conventions. Numerous states prohibit political contributions by corporations. U.S. federal law also prohibits political contributions by persons who are not U.S. citizens or a national of the U.S. and who is not a permanent resident alien. Laws of various jurisdictions, including the U.S., impose various other limitations and restrictions on political contributions. Where corporate political contributions are legal, such contributions shall be made only from funds allocated for such a purpose and must be authorized or verified by the Board of Directors of the contributing entity.

Subject to any further legal limitations, employees may make political contributions to elected officials at the State, County and local levels only if the contributions, in total, are not in excess of $250 by an employee to each official of such issuer, per election. Political contributions to federal elected officials are not subject to this restriction but are subject to the limitations imposed by federal election laws. Non-executive members of the Board of Directors of the Company are not subject to the restrictions of this paragraph; however, it is expected that, at all times, Board Members will comply with any and all state and federal laws regarding political contributions, making reasonable inquiries and contacting the Compliance Director in the case of any uncertainty.

In addition, the Company will not purchase tickets or pay fees for Employees to attend an event where any portion of the funds will be used for election campaigns. Using company time or assets (phone, fax, computer) to support an Employee's run for public office or campaigning for a candidate is the equivalent of such a contribution, and is therefore not permitted. However, reasonable time off without pay, or the use of vacation time to support these activities is permitted. The Company will maintain a "Prohibited List" of state and municipal entities and other public or quasi-public entities ("Prohibited Entities") to take into account special situations and sensitivities concerning certain state and municipal entities. No Employee or director will be permitted to make a donation to a Prohibited Entity, any candidate for office with a Prohibited Entity or a candidate for any office if the candidate is an official with a Prohibited Entity, without the prior approval of the Compliance Director. Any exceptions to the above stated policies must be approved by the Compliance Director. A current version of the Prohibited List will be made available on the on the shared (p://) drive in the Human Resources folder or will be provided to employees and/or directors via email or other means.

P. COMMERCIAL BRIBERY

No commercial bribes or other similar payments or benefits shall be paid directly or indirectly to employees of suppliers or customers.

Commercial bribery includes any payment, or giving any thing of value, direct or indirect, to any director, officer, employee or representative of a customer or supplier of the Company made for the purpose of influencing or affecting such person's business judgment or action.

Q. ANTITRUST AND COMPETITION

The global activities of the Company are subject to antitrust and competition laws of various countries. Employees are required to consult with compliance personnel and internal counsel on all antitrust-sensitive matters.

In general, antitrust and anti-competition laws prohibit agreements or actions that may restrain trade or reduce competition. Violations include agreements among competitors or others to fix or control prices or to allocate territories or markets. Exceptions may exist for lawful joint ventures or regulated activities. Subject to the confirmation by the Compliance Director that there exist any such exceptions, Syncora prohibits Employees from participating in any discussions, understandings or agreements with a competitor regarding:

- Setting, raising, lowering, stabilizing or otherwise affecting premiums, rates, commissions or prices;
- Matters that would affect the availability or terms of insurance or reinsurance coverages or of other services or products;
- Allocation of markets, territories, or potential insureds, reinsureds or other customers;
- Limiting the number of insurers competing to sell insurance;

- Encouragement of a boycott of a person, customer or an insurance product or service or any other product or service, including whether to quote or not to quote certain types or classes or risks;
- What constitutes a "fair" profit level; or
- Credit terms.

Employees are also prohibited from discussing with or providing to any competitor, insurance broker or other third party any artificially inflated bids, prices and/or other terms and conditions with respect to insurance or reinsurance for the purpose of conferring a commercial advantage or disadvantage upon a third party and/or creating a false appearance of legitimate competition within the insurance industry.

R. HEALTH, SAFETY AND ENVIRONMENTAL PROTECTION

The Company will conduct its business in a manner designed to protect the health and safety of its Employees, its customers, the public, and the environment. The Company's policy is to comply with all applicable governmental health, safety, and environmental requirements. Any departure or suspected departure from this policy must be reported promptly.

S. ANTIBOYCOTT

The United States has enacted laws that prohibit or penalize participation in international boycotts not sanctioned by the United States, specifically the Arab boycott of Israel. U.S. law imposes reporting requirements regarding any requests to participate in any such unsanctioned boycott. The U.S. laws apply to entities organized under U.S. law and their controlled foreign affiliates, and to U.S. nationals or residents employed by such entities, but do not apply to U.S. nationals working for a non-U.S. company and residing outside the U.S. All Employees shall refer any request to participate in any such boycott to the Compliance Director in advance of taking any action regarding a request to participate in any such boycott.

T. TRADING RESTRICTIONS

There are a variety of laws restricting trade enacted by countries in which the Company does business and these trade restrictions often apply to insurance and reinsurance activities. These restrictions may apply whether the trading takes place from the United States or otherwise. In all cases, U.S. trade restrictions apply to U.S. citizens and residents no matter where they are located as well as entities organized in the U.S. and persons in the U.S.

The Compliance Director maintains a current list of territories to which U.S., United Nations, European Union or other sanctions apply. These appear on a "Watchlist." Presently, the United States imposes broad restrictions on trade with Syria, Cuba, Sudan, Iran and Myanmar (Burma) (and, more narrowly, the Democratic People's Republic of (North) Korea). Before engaging in

transactions with countries on the watchlist Employees should consult the Compliance Director or a Compliance Attorney to ascertain if governing law prohibits any proposed transactions. This list may change from time to time and current information will be made available to Employees via the intranet or email. In addition, the U.S. Treasury periodically publishes lists of Specially Designated Nationals (SDNs), which are individuals and businesses with whom transactions are prohibited and whose assets in some cases must be blocked by persons subject to the regulations, because the SDNs are allegedly acting on behalf of embargoed countries. List of individuals are also published outside the U.S. by the European Union and the Bank of England. There are also restrictions regarding dealing with designated terrorists, foreign terrorist organizations, narcotics traffickers, narcotics kingpins, entities engaged in money laundering and vessels in which targeted countries have an interest, as well as with designated persons and entities undermining democratic process in Zimbabwe and the Western Balkans. There are also arms embargoes concerning certain countries and restrictions relating to trading in rough diamonds. Transactions involving exports or re-exports to designated entities in India, Pakistan, China, Israel, Russia and Syria are also restricted.

Any Employee contemplating doing business or completing a transaction with nationals or public or private sector entities from such restricted countries or with restricted persons or entities must obtain prior approval from both a manager and the appropriate compliance officer.

U. PROHIBITIONS AGAINST BRIBERY OF GOVERNMENT OFFICIALS AND BOOKS AND RECORDS REQUIREMENTS

Employees who come in contact in the course of their employment with government officials, political parties, party officials, candidates for political office and officials of public international organizations, whether U.S. or foreign, must maintain the highest professional standards. Never offer anything of value to any of the foregoing persons or related parties in an attempt to obtain a particular result for the Company or induce an act or decision by such person in his or her professional capacity. Employees must adhere to all applicable laws and regulations, including, without limitation, the Foreign Corrupt Practices Act.

V. ANTI-MONEY LAUNDERING

Money Laundering is a term used to describe the process of integrating profits from illegal activities into the legitimate financial system so that the profits appear to have originated from a legitimate source. The Company is committed to the prevention and detection of money laundering and may be required by anti-money laundering legislation to implement effective anti-money laundering strategies. Any Employee who knowingly permits illegal conduct or ignores suspicious activity that may indicate money laundering, will be subject to discipline, and can also be subject, along with the Company, to criminal and civil penalties. Money laundering issues are complex and Employees should not attempt to handle them on their own. Employees who have any questions or who become aware of any questionable business activities or

circumstances that could suggest money laundering should promptly consult a compliance officer.

The Company's money laundering training program will include training of new Employees, Employees whose duties could expose them to attempted money laundering (such as Employees responsible for the opening of new accounts), and the superiors of such Employees.

W. PRIVACY

To ensure the confidentiality of any personal information collected and to comply with applicable laws, any Employee in possession of non-public, personal information about the Company's customers, potential customers, or Employees, must maintain the highest degree of confidentiality and must not disclose any personal information, unless authorization is obtained from the Compliance Director. Employees must ensure that electronic data of this nature is protected in transmission and storage through the use of secure email or encryption. In general, the Company applies Data Privacy standards in relation to any data processed that relates to Employees, clients or others. Further, Employees must follow any local privacy standards which are applicable. (See **Appendix D** regarding the Company's Policy with respect to Protecting Personal Information.)

X. DOCUMENT RETENTION

Employees must comply with any documentation directive issued in connection with litigation to which the Company is subject.

Y. TAX GUIDELINES

Syncora companies operate in a number of different jurisdictions throughout the world and are subject to oversight by various tax regulatory bodies. Employees must be aware of, and adhere to the Company's tax procedures and protocols as promulgated by Syncora from time to time. All inquiries relating to tax should be referred to Syncora's tax advisors (both internal and external).

Z. ELEVATED RISK COMPLEX STRUCTURED TRANSACTIONS

Syncora has established and maintains, on a firm-wide basis, policies and procedures that are designed to accord increased scrutiny to any transactions entered into by the Company which pose elevated levels of legal or reputation risk to Syncora ("Elevated Risk Complex Structured Transactions"). Among other things, the policies help the Company identify, evaluate, address and manage these risks within its existing control framework. Examples of transactions that require heightened analysis include, among others, transactions that appear to:

- Lack economic substance or business purpose;

- Are designed for questionable accounting, regulatory or tax objectives;
- Raise concerns that the client will report or disclose the transaction in its public filings or financial statements in a manner that is materially misleading or inconsistent with the substance of the transaction or applicable regulatory or accounting requirements.

Any Employee who is presented with an Elevated Risk Complex Structured Transaction must conduct appropriate due diligence and take appropriate steps to address the risks from the transaction. Any concerns regarding Elevated Risk Complex Transactions should be referred to the Compliance Director.

COMPLIANCE CONTACTS INFORMATION FOR SYNCORA HOLDINGS LTD. AND ITS SUBSIDIARIES AND AFFILIATES

COMPLIANCE DIRECTOR

NAME	TELEPHONE	FAX
James W. Lundy, Jr.	212-478-3405	212-478-3579

LEGAL DEPARTMENT

NAME	LOCATION	TELEPHONE	FAX
Matthew Morse	New York	212-478-3410	212-478-3579

REGULATORY COMPLIANCE

Regulatory compliance is overseen at a regulated entity level with each regulated entity having designated regulatory compliance staff or resources available to it.

APPENDIX A

SYNCORA HOLDINGS LTD.

CODE OF ETHICS FOR SYNCORA SENIOR FINANCIAL OFFICERS

Financial Officers throughout Syncora Holdings Ltd. and its consolidated subsidiaries (the "Company") play a critical role both in (1) the financial and management reporting process to Executive Management, the Board of Directors and Committees thereof, shareholders, and various regulatory and governmental agencies; and (2) the Company's internal controls.

The financial reporting process encompasses the accuracy of the accounting books and records, accurate preparation of financial statements, the establishment of accounting procedures and internal accounting controls including the proper authorization for transactions and the safeguarding of assets and appropriate recognition of liability, and the accuracy of financial information utilized to manage the business activities and affairs and related financial disclosures to shareholders and regulatory authorities.

The activities of financial officers within the Company are governed by a number of applicable laws, regulations and standards, including various local governmental and quasi-governmental agencies including - SEC, FASB, National Association of Insurance Commissioners, NY Insurance Department, Financial Supervisory Authority of the UK, International Accounting Standards Board, etc.

Certificate of Compliance

In recognition of a duty of care and loyalty to the Company as a whole and that the Board of Directors of the Company speaks for the company, Financial Officers of the Company, to fulfill their responsibilities to the Company's financial reporting process and system of internal control, will certify as follows:

"I, _____, as a Financial Officer of Syncora Holdings Ltd. or one of its consolidated subsidiaries (the "Company") hereby certify that I will:

1. Comply with the Syncora Holdings Ltd. Code of Business Conduct and Ethics.
2. Act with honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships, which could be reasonably determined to harm the Company's reputation.
3. Apply accounting policies that are appropriate to the proper recording of transactions, including the proper timing of revenue and expense recognition.
4. Ensure critical accounting policies are in accordance with those adopted by the Company and communicated by the Corporate CFO/Corporate Controller.
5. Ensure that internal controls over the financial reporting process is maintained to a high professional standard and deficiencies are timely corrected.

6. Establish and maintain a comprehensive financial reporting process to support internal management decision-making needs and external filing requirements.
7. Provide constituents with information that is accurate, complete, objective, relevant, timely and understandable.
8. Comply with rules and regulations of federal, state, provincial and local governments, and other appropriate private and public regulatory agencies.
9. Act in good faith, responsibly, with due care, competence and diligence, without misrepresenting material facts or allowing one's independent judgment to be subordinated.
10. Respect the confidentiality of information acquired in the course of one's work except when authorized or otherwise legally obligated to disclose. Ensure confidential information acquired in the course of one's work will not be used for personal advantage.
11. Share knowledge and maintain skills important and relevant to Company's needs including formal or informal education and training as appropriate.
12. Promote ethical behavior as a responsible partner among peers, in the work environment and the community.
13. Achieve responsible use of and control over all assets and resources employed or entrusted.
14. Ensure all liabilities and contingent liabilities, including commitments and guarantees, are properly recorded.
15. Comply with policy rules pertaining to non-audit services provided by our independent auditors.
16. Ensure appropriate record retention policies are in place for the financial reporting process and to satisfy all regulatory requirements.
17. Cooperate fully with all internal and external auditors and appropriate regulatory authorities.
18. Avoid taking any action to fraudulently influence, coerce, manipulate or mislead independent auditors.

Signed by: _____
Printed name: _____
Date: _____"

APPENDIX B

PROCEDURES FOR APPROVAL OF RELATED PERSON TRANSACTIONS

Related Person Transaction Guidelines

With respect to any proposed Related Person Transactions[1] (as defined below), Syncora Holdings Ltd. together with its subsidiaries (collectively, the "Company" or "SHL") shall adhere to the following Related Person Transaction Guidelines (the "Guidelines"):

- Company management shall submit to the Nominating & Governance Committee any Related Person Transaction (other than Ordinary Course Related Party Transactions and SCAI Related Party Transactions) for its review. In reviewing proposed Related Person Transactions, the Nominating & Governance Committee shall consider, among other things, if such transactions are on terms comparable to those that could be obtained in arm's length dealings with unrelated third parties and shall review such transactions to determine that the terms are arm's length or otherwise fair to the Company.

- After its review of a proposed Related Person Transaction, the Nominating & Governance Committee shall approve or disapprove such proposed transaction.

- If action must be taken with respect to a proposed Related Person Transaction (other than an Ordinary Course Related Person Transaction or an SCAI Related Party Transaction) prior to the next regularly scheduled Nominating & Governance meeting, a member of Company management will so inform the Company's Chairman of the Board and the Chairman of the Nominating & Governance Committee. An e-mail will then be sent by Company management to the Company's Chairman of the Board and to all members of the Nominating & Governance Committee providing the details of the proposed Related Party Transaction. All recipients of the e-mail will be given five business days to respond with any issues or questions they have regarding the proposed transaction. If no issues or

[1] Under the 2009 MTA, Syncora Guarantee Inc. ("SGI") and Syncora Capital Assurance Inc. ('SCAI") are each prohibited from entering into transactions with each other (or for the benefit of each other), or any Affiliate (as such term is defined in the 2009 MTA) unless such transactions are entered into pursuant to the terms of existing agreements between the parties (such as pre-existing reinsurance agreements). As such, any Related Person Transaction between SGI and SCAI, and/or any Affiliate, would have to qualify under these Related Person Transaction Guidelines and the terms of the 2009 MTA. In addition, most transactions between insurance affiliates would require approval of the New York State Department of Financial Services under Section 1505 of the New York Insurance Laws.

questions are raised within such five business day period, Company management may then approve the proposed Related Person Transaction. A Related Person Transaction so approved shall then be ratified by the Nominating & Governance Committee at the next scheduled Nominating & Governance Committee meeting. Notwithstanding the foregoing, depending on the nature of the Related Person Transaction, the Chairman of the Nominating & Governance Committee may determine that a meeting of the Nominating & Governance is preferable to an e-mail exchange in which case a meeting of the Nominating & Governance Committee will be scheduled accordingly.

- Any Ordinary Course Related Person Transaction may be approved by Company management and it is not necessary for such transactions to be presented to the Nominating & Governance Committee for prior approval.

- At each meeting of the Nominating & Governance Committee, Company management shall update the Nominating & Governance Committee as to whether there have been any material changes to any of the Related Person Transactions that it has previously approved.

- No Director may participate in any discussion or approval of any Related Person Transaction for which he or she is a Related Person.

- On an annual basis, Company management will provide to the Nominating & Governance Committee a list of all existing Related Person Transactions and, if applicable, the volume of business transacted thereunder.

- SCAI Related Person Transactions: any Related Person Transactions for which SCAI is a party shall be brought before SCAI's Special Transaction Committee for approval and shall not require the separate approval of the Nominating & Governance Committee.

Defined Terms. Within these Guidelines, the following words and phrases shall have the meanings given to them below:

"SCAI Special Transaction Committee" means the special committee established for SCAI that has veto power over transactions between SCAI and SHL and transactions between SCAI and Syncora Guarantee Inc. ("SGI"), established pursuant to the Master Transaction Agreement, dated April 26, 2009, among SHL, SGI and certain of its affiliates and counterparties to credit default swap agreements with SGI and affiliates party thereto.

"Director" means a member of the Company's Board of Directors.

"Nominating & Governance Committee" means the Company's Nominating & Governance Committee.

"Ordinary Course Related Person Transaction" means a Related Person Transaction that is entered into under an existing reinsurance agreement, master services agreement, general services agreement or other similar agreement that is currently in place as of December 1, 2009 or approved by the Company's Nominating & Governance Committee.

"Related Person" means an executive officer, Director or nominee for director of the Company, a greater than 5% beneficial owner of the Company's outstanding Common Shares, any immediate family member (as that term is defined by Item 404 of Regulation S-K) of any of the foregoing or an entity in which a person listed in the foregoing has a substantial interest in, or control of, such entity or which employs a person listed in the foregoing.

"Related Person Transaction" means any transaction, including a proposed charitable contribution or pledge of charitable contributions, in which the Company was or is a participant, and the amount involved exceeds $100,000 and in which a Related Person had or will have a direct or indirect interest.

APPENDIX C

SYNCORA DESIGNATED DIRECTORS SERVING ON THE BOARDS OF SYNCORA AFFILIATED COMPANIES

1) An "Affiliated Company" is defined for this purpose to include any company (a) in which Syncora Holdings Ltd. or a subsidiary thereof (herein "Syncora") owns or controls at least 5% but less than 50% of the common equity share capital and/or the voting share capital of such company on a fully diluted basis or (b) where Syncora has a joint venture or a major strategic alliance arrangement with such company.

2) Companies in which Syncora controls more than 50% of the common equity share capital and/or the voting share capital are treated under the Syncora policies governing subsidiary companies.

3) An Affiliated Company may either be publicly traded or privately held.

4) The Chairman of the Board and the Chief Executive Officer of Syncora may each designate officers or other employees of Syncora ("Syncora Designee") to serve from time to time as members of boards of directors of Affiliated Companies, subject to approval or ratification by the Board of Directors of Syncora and confirmation by such Board that such persons are serving at the request of Syncora.

5) Syncora Designees serving as directors of Affiliated Companies may not receive any "director compensation" (as defined below) from Affiliated Companies which are privately held without the prior approval of the Nominating and Governance Committee of the Board of Syncora ("Nominating and Governance Committee").

6) If the Nominating and Governance Committee provides its prior approval in accordance with Paragraph 5 above, any director compensation otherwise payable to any Syncora Designee serving as a director of an Affiliated Company that is privately held is to be promptly transmitted to Syncora (Attention — Corporate Controller). Any Syncora Designee receiving such approval shall be responsible for ensuring that the Corporate Controller and the General Counsel of Syncora are informed of the nature and timing of the payments of such director compensation.

7) Syncora Designees serving as directors of Affiliated Companies that are publicly traded must waive their right to receive any director compensation from such Affiliated Companies. Any such Syncora Designee shall be responsible for ensuring that the General Counsel or other appropriate legal counsel reviews and approves all aspects of such waiver on an annual basis (including any potential disclosure in the Affiliated Companies' proxy statement or other public documents relating to director compensation and any waiver thereof by such Syncora Designee).

8) "Director compensation" is defined broadly to include cash retainers and committee fees, stock options, restricted stock and phantom stock units. In cases where director compensation is paid and there is an option for a deferred payment mechanism such mechanism should not be availed of.

9) Syncora shall keep current a schedule of all Syncora Affiliated Company directorships on an annual basis and each Syncora Designee and each of the Chairman, the Chief Executive Officer and the General Counsel of Syncora shall promptly report all changes regarding such directorships to the Secretary in order to facilitate the collection of such information.

APPENDIX D

END USER INFORMATION RISK MANAGEMENT POLICY

OVERVIEW

The information created, processed, and used by Syncora is one of our most valuable assets. A compromise of these information assets could severely impact our customers, constitute a breach of laws and/or regulations, and may negatively affect the reputation and revenues of Syncora. An effective information risk management program is a team effort involving the participation of every individual who deals with or has access to Syncora information and/or Syncora information systems. It is the responsibility of every User (as defined below) to know this policy, and to conduct their activities accordingly.

SCOPE

This policy outlines the minimum standards set for Information Risk Management that must be followed by all Users who access Syncora information or use Syncora IT resources. These rules are in place to protect the Users and Syncora. Inappropriate use of Syncora information or IT resources exposes Syncora to risks including malware, spyware and virus attacks, compromise of network systems and services, legal and regulatory issues, and third party claims.

This policy applies to users[4] of all equipment that is owned or leased by Syncora (the "User" or "Users"). This includes, but is not limited to: systems, software, storage media including printed output, databases, terminals, fax machines, voice mail, electronic mail (E-Mail), networks, personal computers, mobile devices (which should be read to include laptops, smart phones and tablets), Internet, and Intranet.

Responsibility

The safeguarding of Syncora information assets is every User's responsibility. All Users **must**:

- Maintain the confidentiality of customer and Syncora information.
- Ensure as far as practical that customer and Syncora information is accurate and ensure that it is kept secure.

[4] Includes employees, consultants, vendors and advisors

- Adhere to all security, electronic communication, and confidentiality policies as mandated by the Code of Business Conduct & Ethics.

- Immediately report any violation of this policy or known security incident to the Chief Administrative Officer or Compliance Director.

IT Security

1. All Users are required to authenticate their identity prior to initiating a computer session or electronically accessing Syncora information. The required means of identification for most systems and applications will be a unique User ID and password. For remote access (for example gotomypc) the required process will include an additional unique user password (multi-factor authentication).

2. Passwords are confidential and must **never** be shared, made known to others or written down. Passwords should not be displayed or echoed in clear text on the screen. It is the responsibility of each user to protect his or her password. Users are fully accountable for **all activity** associated with their User ID and password.

3. In order to preserve the integrity of Syncora information systems, Users are required to abide by the following construction rules when selecting a password:

    - Passwords must consist of a minimum combination of eight (8) mixed alpha and numeric characters.

    - Passwords must never be the same as or contain the User ID.

    - Passwords should not contain more than two consecutive, identical characters.

    - Passwords must not be reused until after at least four iterations, i.e. users should not select the same password until they have rotated through five other passwords.

    - Passwords should not be selected in a way that makes them easy to guess. For example, it is best practice to never use personal details (family name, license plate), obvious dates (birthday, anniversary), generic text (Syncora, Bermuda), or words found in a dictionary.

4. Users should change their password(s) immediately if they suspect that they have been compromised or if they notice anything unusual about their computer system. The User should also contact the IT Help Desk if this situation occurs. Regardless, all users will be required to change the password on Syncora devices every ninety (90) days.

5. Users must either lock their workstation or activate their password protected screen saver when leaving their workstation or mobile device unattended.

6. Users are required to log off their workstation at the end of the workday unless it is running an overnight process, in which case the screen saver should be activated.

7. Laptops must be physically secured when not in use and should never be left unattended in public places.

Data and Software Security

1. Users are prohibited from loading unlicensed or unauthorized software onto any Syncora owned or leased PC, workstation, or mobile device. Users are also prohibited from downloading software from the Internet unless required for specific business purposes and with the approval of their manager and the IT Department.

2. Users may not allow Syncora owned or licensed software or other intellectual property to be copied by others and may not themselves make copies other than those provided for in the relevant licensing agreements.

3. Users may not load Syncora owned or licensed software or other intellectual property onto any device not owned or managed by Syncora. This is includes personal home computers, CDs, DVD, and USB devices.

4. Users must not use personal email accounts (e.g. Yahoo, hotmail, gmail, etc.) to conduct Syncora business unless approved by the Compliance Director. This includes sending Syncora email to/from home email accounts.

5. Users must not send Syncora confidential data including personally identifiable information to external parties without protecting the data through the use of secure email, password protected files, or other encryption methodologies as approved by Syncora IT Security.

6. All hardware, software, and IT resources supplied by Syncora are the property of Syncora and as such may at any time, without prior notice, be subject to audit review.

7. Users may not access any information system or information contained on Syncora systems without proper authorization, nor may they make any modifications to said contents without appropriate entitlement rights.

8. Users are responsible for the integrity, confidentiality, and availability of Syncora data contained on their PC, workstation, or other mobile device and all forms of removable media (CD, DVD, USB device, etc.). Users should request assistance from the IT Help Desk if they are unsure whether they are adequately securing their data.

9. Information Owners should clearly label confidential information or make certain that Users are aware of its classification.

10. Users should ensure that they do not inadvertently disclose confidential or sensitive information, for example by printing it to an unattended printer or fax machine.

Network Security

1. Users should not connect to any third party (i.e. Internet, Extranet) while connected to Syncora networks except through Syncora authorized gateways.

2. Users are prohibited from connecting personally owned computers or other mobile device to the Syncora network except through a service authorised by the Company and the IT department . Any device other than Syncora issued equipment is considered unauthorized.

Anti Virus Security

1. Any software or data received from any external source, including the original manufacturer and the Internet, should be treated as suspect and not installed, executed or used in any other fashion until it has been scanned for viruses using Syncora's virus detection software; the IT Help Desk should be contacted to perform the installation.

2. Any actual or suspected virus related problem should be reported **immediately** to the IT Help Desk. In particular, Users should never forward virus warnings received from any external source as they may spread a virus or perpetuate a virus hoax.

3. Laptop and standalone PC Users are responsible for checking that the automated updating of their anti-virus software is functioning properly. Should it not be functioning correctly the user should contact the IT Help Desk immediately.

Physical Security

1. Users should take all reasonable steps to ensure that all Syncora equipment in their possession or under their control is protected at all times against theft, accidental or deliberate damage by others and damage by natural elements.

2. Lost, stolen or damaged Syncora equipment should be reported to the IT Help Desk as soon as possible.

3. Any Syncora equipment other than the individual's mobile device(s) taken off site must have management authorization for removal.

4. Do not permit people to gain access to restricted areas by following you through security doors and other mechanisms. Keep all access devices in a safe place. Users are responsible for the consequences of permitting people to gain access to restricted areas but, in all cases, access to IT-sensitive areas (e.g. the LAN room) should only be provided by members of the executive management team, a member of the IT team or the company's Facilities Manager.

Information Storage

Syncora information must be protected regardless of the media upon which it is maintained. This includes, but is not limited to, the following types of media: CD, DVD, USB device,

diskette, hard copy output, magnetic disk, microfilm, microfiche, optical disk or paper documents.

Clean Desk Policy

Users should practice a clean desk program by protecting confidential information stored on any media from unauthorized access while it is in their custody.

1. All documents, folders and other storage media containing confidential information should not be left on desks or in storage areas when unattended or unmonitored.

2. All media containing confidential information should be secured at the end of each workday.

3. All papers should be removed and boards should be wiped when finished using conference rooms.

Useful Life

Confidential information should be maintained in accordance with our Document Retention and Destruction policy. Information that must be destroyed in accordance with this policy, should be destroyed in a manner that renders it unusable and unrecoverable[5].

- Paper media should be disposed of using paper shredders or secure trash disposal providers.

- Electronic media must use secure delete, physical destruction or degaussing processes.

Definition of "Personal Information"

From time to time, the Company may collect various personal information regarding its employees or others, either to provide services or as required by law. "Personal Information" is information that can be associated with a specific person and/or is used for such purposes as obtaining credit, obtaining public or private benefits or accessing secured sources of information. "Personal information" may include any of the following types of information: social security numbers; home address and telephone information; personal email addresses and passwords; driver's license and state-issued ID numbers; bank or financial account numbers, PIN numbers and passwords; credit and debit card numbers; passport or alien registration numbers; medical information; health insurance ID numbers; or an individual's maiden or pre-marital name.

---

[5] All users must comply with issued data preservation directives; such directives supersede the Company's Document Retention and Destruction policy.

Protection of Personal Information

The Company has adopted policies to protect any personal information that it collects. Specifically the Company will:

- collect only the minimum amount of personal information that is necessary for it to provide services or that it is required to collect by law, and provide a secure means of collecting that information;

- retain personal information only on secured servers or in secure physical storage;

- limit access to personal information only to individuals who require that information in order to provide services or perform administrative tasks relating to employees, and do not disclose such information except as required by law or legal process;

- train individuals who have access to personal information to (i) maintain such information securely at all times, and (ii) where such information must be transmitted to a third party, transmit it in a secure fashion; and

- dispose of personal information that is no longer needed for any business purpose securely, so that it cannot be accessed by others.

Individuals who violate any aspect of this policy may be subject to disciplinary action, up to and including termination of employment.

COMPLIANCE

Use of Syncora Information on Syncora IT Resources as set out in this policy may be monitored by Syncora for compliance to this policy. All violations will be brought to the attention of the Employee's manager, Human Resources and the Compliance Director for appropriate disciplinary action, which may result in revocation of information access, and possible disciplinary action up to and including termination.