Code of Business Conduct

February 2019

TABLE OF CONTENTS

Page

WATFORD HOLDINGS LTD.
Code of Business Conduct

GENERAL STATEMENT

Watford Holdings Ltd. ("WHL") and its subsidiaries[1] (together with WHL, the "Company") are committed to integrity in the conduct of their business and require that all Employees (as defined below) perform their duties in a manner which is legally, ethically and morally irreproachable. Our Board of Directors and senior management have made the development of an organizational culture that encourages compliance with the highest ethical standards one of our first priorities. The Company's standards are clear: simply complying with laws or following widespread business practices may be insufficient.

To implement WHL's commitment to integrity in the conduct of our business, we have adopted a Code of Business Conduct and an included series of policy statements to provide clarification and, where applicable, detail regarding certain aspects of the Code of Conduct (the "Policy Statements," and collectively with the Code of Conduct, the "Code," of which the Policy Statements are considered an integral part). The Company's goal, in promulgating the Code, is to ensure that we have in place policies and systems designed to prevent and detect violations of our Code and to be able to respond appropriately to any violations and to prevent further violations.

The Code describes the ethical principles the Company has set for the conduct of its business, and outline certain key legal requirements of which all Employees should be generally aware. Compliance with these requirements, together with any additional requirements applicable to any subsidiary, branch or other local operation of the Company under applicable local laws, is mandatory. While adherence to the principles set forth herein is a condition of employment at the Company, no employment contract is intended or offered by reason of this Code. Violations will not be tolerated and may result in one or more of the following: warnings, reprimands, probation, demotion, temporary suspension, reimbursement of the Company's losses or damages, discharge or any other actions as may be appropriate. Please note that a violation of the Code may, under certain circumstances, also constitute a criminal act which may require the Company to start legal action against such violators or refer such violation to appropriate law enforcement authorities.

The Code identifies conduct which is never acceptable and which will always be considered outside the scope of your employment. It is therefore crucial that each Employee read and understand the information presented in this Code.

---

1 See Schedule I for a current list of WHL subsidiaries, all of which are subject to the Code.

SCOPE

The Code applies to all of our officers, all persons employed directly by the Company and, where relevant, our directors ("Employees"). In addition, where appropriate, the Company will also require certain agents of the Company to comply with the Code and to certify their compliance in the same manner as if they were Employees.

For the avoidance of doubt, for purposes of this Code, employees of Arch Underwriters Ltd. ("AUL") and Arch Underwriters Inc. ("AUI") or their affiliates made available to the Company on a non-exclusive basis pursuant to those certain Services Agreements between the Company and AUL or AUI as appropriate (and as may be amended or supplemented) shall not be deemed to be Employees of the Company and shall instead be deemed to be agents and representatives of the Company when acting on the Company's behalf.

For purposes of complying with this annual certification requirement, any employees of Arch Capital Group Ltd and its subsidiaries (collectively, "Arch") who perform services for the Company or on the Company's behalf will satisfy this requirement through annual certification to Arch that they are in compliance with the Arch Code of Conduct and related Policy Statements, which the Company expressly deems equivalent to this Code.

The Company expressly acknowledges that the non-Employee directors of Watford Insurance Company Europe Ltd. ("WICE") are also directors of other for-profit entities, and relies upon their good judgment in discharging their duties to the Company. Non-Employee directors and officers of WICE shall be deemed to be agents and representatives of the Company when acting on the Company's behalf, and shall be required to adhere to the requirements of this Code and to annually certify their compliance to the Director of Compliance or his designee.

RESPONSIBILITIES

It is the responsibility of each Employee to conduct himself or herself in a manner that will support and maintain the Company's reputation for fairness and a high level of integrity. As representatives of the Company, it is essential that Employees' actions are legal and ethical. It is equally important that no actions taken by an Employee appear to others to be inconsistent with that high standard. In every case, an Employee should ask himself or herself if the conduct being contemplated would comply with Company policies and would withstand public disclosure and scrutiny. By doing business in this manner, we can ensure the respect of our clients, shareholders, fellow Employees, regulatory authorities, governments and neighbors.

ACKNOWLEDGMENT AND CERTIFICATION

The Code supersedes any pre-existing policy statement covering the same or similar subject matter. Every Employee must annually sign a Certificate of Compliance certifying that he/she has received, reviewed and understands the Code and agrees to comply therewith. The required Certificate of Compliance, which must be signed and returned to the Director of Compliance or his/her designee, accompanies this document.

ADMINISTRATION OF THE CODE

Overall responsibility for the administration of the Company's Code and education related thereto has been assigned to the Chief Operating Officer of WHL, who functions as the Director of Compliance. The Director of Compliance may consult with other personnel as deemed appropriate and necessary to ensure the proper administration of the Code. The Director of Compliance may also, in its discretion, determine to consult with the Company's outside counsel on any of the matters arising within this Code or any of the included Policy Statements. The Director of Compliance may designate a compliance contact for some of the Company's operating subsidiaries, and any such subsidiary compliance contacts will coordinate with the Director of Compliance. The names, addresses, titles, telephone numbers and e-mail addresses of each of the persons currently designated as Director of Compliance and subsidiary compliance contacts are attached as Schedule II to this Code. To the extent a subsidiary does not have a designated compliance contact, Employees should contact the Director of Compliance directly.

QUESTIONS AND REPORTING

If you see any actual or proposed business conduct by an Employee or anyone doing business with the Company, which you in good faith believe constitutes a violation of the Company's Code or any applicable law or regulation, or if you have any questions in that regard, or if you are aware of situations which could implicate the Company in unlawful conduct by others, you have an obligation and you are encouraged to come forward. When in doubt, ask before you act. You may bring any question you may have or report any questionable conduct to the Director of Compliance or your subsidiary compliance contact, or their designees, or take advantage of the Compliance Hotline which has been established by the Company. The Compliance Hotline telephone numbers appear in Schedule II attached to this Code. To the extent practicable under the circumstances, all reasonable steps will be taken to keep confidential the identity of anyone reporting a violation. Your communications will be taken seriously and, if warranted, the matter will be investigated.

The Compliance Hotline will record all calls and it is the responsibility of the Director of Compliance to determine what action, if any, is appropriate. Calls to the Compliance Hotline may be made anonymously if desired.

The Company will protect Employees from negative consequences that may result from fulfilling their reporting obligations. The Company will not discharge, suspend, demote or take adverse employment action against an Employee who believes and communicates in good faith that a policy or practice is in violation of applicable laws, rules or regulations simply because an Employee makes any such report, unless the Employee has been a willful participant in the wrongdoing, has allowed or encouraged the violation to occur or has otherwise committed misconduct. This policy is intended to encourage Employees to come forward and report violations. We encourage Employees to disclose their own violations of any applicable law, regulation or Company policy. While we cannot promise in advance that Employees who report their

own violation of any applicable law, regulation or ethical standard will not be disciplined or otherwise dealt with by appropriate authorities, we intend to apply any discipline in a fair and equitable manner.

TRAINING

To ensure that all Employees understand their responsibilities under the Code, as required the Director of Compliance, or his/her designee, and the subsidiary compliance designees, if any, may determine to develop training programs to facilitate compliance with the Code. New Employees will receive an introductory briefing from the Director of Compliance or the relevant subsidiary compliance designee on the principles of the Code as part of their orientation. To the extent needed, the Company will arrange additional specialized training for any Employees whose responsibilities involve compliance with the laws, regulations or standards of conduct applicable to our operations.

PROCEDURES REGARDING WAIVERS

Because of the importance of the matters involved in this Code, waivers will be granted only in limited circumstances and where the circumstances would support a waiver. Waivers of the Code may be made only by the Director of Compliance. However, waivers of the Code for executive officers or directors of WHL may only be made by the Board of Directors. If and to the extent WHL becomes subject to the reporting requirements under the Securities Exchange Act of 1934 (the "Exchange Act"), any waiver granted to the executive officers or directors of WHL must be publicly disclosed on WHL's website or on Form 8-K to the extent required by the U.S. securities laws or the rules and regulations of any exchange applicable to us.

1. HONEST AND FAIR DEALING

Employees must endeavor to deal honestly, ethically and fairly with the Company's customers, suppliers, competitors and Employees. No Employee should take unfair advantage of anyone through manipulation, concealment, abuse of 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 rise to a level of fraud and thereby expose Employees and the Company to criminal and/or civil liability for violation of anti-fraud laws, as well as the antitrust laws. For example, prosecutors and private civil litigants have alleged fraud and other claims in connection with the submission by carriers of sham coverage quotes that reflect higher premiums and/or less favorable terms and conditions than the quotes submitted by the incumbent carriers, where the non-incumbent

carriers' quotes were knowingly provided to assist the incumbent carriers in retaining the clients' business.

2. CONFLICTS OF INTEREST

Each Employee owes a duty of loyalty to the Company. For that reason, all Employees must exercise great care any time their personal interests conflict with those of the Company. Conflicts of interest are to be scrupulously avoided and, if unavoidable, must be disclosed by Employees at the earliest opportunity. A conflict of interest exists if your actions as an Employee are, or could reasonably appear to be, influenced, directly or indirectly, by personal considerations or by actual or potential personal benefit or gain.

In general, without authorization from the Board of Directors or the Director of Compliance, Employees should not own, directly or indirectly, a significant financial interest in any organization conducting or seeking to conduct business with the Company in a manner which is more than merely incidental or immaterial. A significant financial interest is one which is so substantial as to create a potential risk of interference with such individual's independent exercise of judgment in the interest of the Company. Employees who deal with the Company's suppliers are placed in a special position of trust which requires great caution. No Employee should ever receive a payment or anything of value in exchange for a purchasing decision, except for normal business entertainment and tokens of limited value.

No Employee of the Company shall participate on behalf of the Company in any negotiations or dealings of any sort with any person, firm, or non-affiliated corporation in which he/she has, directly or indirectly, an interest, whether through a personal relationship which would affect his or her decisions, or through stockholding or otherwise, other than ordinary investment disclosed to the Company and in any event not sufficient to in any way affect his/her judgment, conduct, or attitude in the matter, or give him/her a personal interest therein.

No Employee shall knowingly compete or aid or advise any person, firm, or corporation in competing with the Company in any way, or engage in any activity in which his/her personal interests in any manner conflict, or might conflict, with those of the Company.

The Company requires the full attention of its employees. In general, this level of attention makes it impractical for employees to pursue employment outside the Company. Additionally, outside employment also could lead to a conflict of interest for the employee.

The same conclusion applies to an Employee serving on the Board of Directors of another company. Consequently, any outside employment or holding the position of director of another corporation by any Employee must be approved in advance by the Director of Compliance, or his/her designee. This requirement shall not apply to an Employee'ss holding the position of director of a not-for-profit entity. However, any non-Employee director of the Company must notify the Board of Directors in the event that he or she holds the position of director of another for-profit entity. The Company expressly acknowledges that any Arch designees to the Company Board of Directors have a duty to Arch as well as to the Company, and relies upon

their good judgment in discharging their duties to the Company. The Company also expressly acknowledges that the non-Employee directors of Watford Insurance Company Europe Ltd. are also directors of other for-profit entities.

Unless expressly authorized or sponsored by the Company, no outside activities should involve the use of the Company's time, name, influence, assets, funds, materials, facilities or Employees.

Employees are prohibited from diverting for personal gain any business opportunity from which the Company might profit unless the Company validly decides to forego the opportunity. You must direct all questions regarding this subject to the Director of Compliance, or his/her designee.

3. ENTERTAINMENT, GIFTS AND PAYMENTS (NON-GOVERNMENTAL AND GOVERNMENTAL PERSONNEL)

The Company and any persons acting on its behalf, will procure goods and services and will sell its products and services on an impartial basis, free from outside influence. Business transactions should always be free from even a perception that favorable treatment was sought, received or given as the result of furnishing or receiving any financial or other advantage, including gifts, favors, hospitality, entertainment or other similar gratuity.

Any financial or other advantage, including payments or things of value, directly or indirectly, to any director, officer, employee or representative of any actual or prospective customer or supplier of the Company, given for the purpose of influencing or affecting such person's business judgment or action, such as to induce the purchase or sale of goods or services, or to induce them to act improperly in any way, 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.

Non-governmental personnel

Employees, or any person acting on behalf of the Company, shall not seek or accept any financial or other advantage, including personal gifts, payments, fees, services, valuable privileges, vacations, or pleasure trips without a business purpose, loans (other than conventional loans from lending institutions), or other favors 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 referral of third parties to any such person or business organization.

Notwithstanding the previous paragraph, gifts to or from non-governmental personnel with whom the Company does or seeks to do business should not exceed U.S. $400 per person or entity in a calendar year. Employees should make good faith estimates of the value of gifts which they receive. Employees may give such gifts provided receipt of gifts is not prohibited by the recipient's employer and regardless of value, there is no intention to induce the recipient to

act improperly in any way. In any case where an Employee receives a gift which is believed to be in excess of this limitation, the Employee should return the gift with a polite note explaining the Company policy.

For this purpose "gift" does not include providing or accepting meals and entertainment of reasonable value motivated by commonly accepted business courtesies, provided such meals or entertainment would not likely cause favoritism or a sense of obligation to the donor or induce the recipient to act improperly. Lavish or excessive meals or entertainment, or meals or entertainment involving the same customer or supplier on a recurring basis, should be avoided.

It is difficult to promulgate a rule as to what is "reasonable" or what is "commonly accepted business courtesy" to cover all circumstances. Employees are urged to make good faith judgments. A good test is — would you be embarrassed if your giving or receiving meals or entertainment were the subject of an article in the Wall Street Journal? In all matters, but particularly in cases of giving or receiving gifts, Employees must be alert to federal or state prohibitions applicable to particular businesses or lines of insurance.

Governmental personnel

Gifts to U.S. or foreign governmental personnel, including public officials, should not be made, regardless of value, unless cleared in advance with the Director of Compliance.

In the United States, there are stringent federal restrictions on the provision of gifts, meals and entertainment to government officials and advance approval from the Director of Compliance or his/her designee is required. There are similar restrictions in numerous states and you must consult with the Director of Compliance or his/her designee in advance of providing gifts, meals and entertainment to State officials.

In jurisdictions outside the United States, gifts may not be provided to government officials without the express approval of the Director of Compliance or his/her designee. Meals and entertainment may be provided to government officials only if permissible under the host country laws and the laws of the country in which the Employee who offers such meals or entertainment is located, and the meals and entertainment must be modest in nature and not provided on a recurring basis.

Violations of this prohibition anywhere in the world may subject the Company and any involved Employees or agents of the Company to severe penalties under the laws of Bermuda, the United States, the United Kingdom and many foreign jurisdictions in which the Company does business.

You are urged to consult with the Director of Compliance or his/her designee if you have any questions regarding this policy.

4. PROTECTION OF PROPRIETARY AND CONFIDENTIAL INFORMATION AND PRIVACY

Proprietary information, that is, nonpublic information which if disclosed outside the Company could disadvantage the Company competitively or financially or which could hurt or embarrass Employees, customers, insurance claimants, suppliers or the Company, must be kept confidential. In addition to maintaining the confidentiality of our own proprietary information, our policy is to respect the proprietary information of others. Indeed, the theft of another's proprietary information is a crime in most jurisdictions. See the Company's "Policy Statement on Confidential Information," which is attached as Appendix A of this Code and the "Policy Statement on Insider Trading," which is attached as Appendix E of this Code.

The Company's services reach deep into the personal and business lives of others, who trust us to protect their privacy. Violating that privacy may result in serious criminal charges and civil liability for both the Company and the Employee responsible. It is the Company's policy to collect and process all personal data in accordance with the applicable privacy laws in each relevant jurisdiction. Every Employee should do his/her utmost to protect the privacy of all forms of business communications, whether voice, data or image transmissions. The United States, Bermuda, Canada and numerous European countries have adopted regulations to ensure the confidentiality of personally identifiable financial and other information. In the United States, financial institutions may not disclose such information to a nonaffiliated third party unless the institution has clearly disclosed to the individual that such information may be disclosed and is provided an opportunity, in advance of the disclosure, for the individual to direct that the information not be disclosed to a third party. Notice of the policies and practices with respect to disclosure shall be provided at the time of establishment of the relationship and annually during its continuation.

The Company policy is that personal data should be processed only by Employees who need the data to perform their jobs and in accordance with any local data protection laws and regulations. Personal data that is no longer needed should be destroyed consistent with such record retention policies as may be adopted from time to time. In some jurisdictions, personal data may be transferred only in limited circumstances, for example upon consent, or if consent may be presumed based on the circumstances or if required to do so by law. Any Employee who receives an inquiry from any party outside the Company seeking nonpublic information regarding the Company, its Employees, customers, insurance claimants or suppliers must refer such inquiries to the Director of Compliance or his respective designees.

5. INTEGRITY OF RECORDS, ACCOUNTING PROCEDURES AND DOCUMENT RETENTION POLICY AND PROCEDURES

Accuracy and reliability of our financial and business records is critically important to the Company's decision-making process and to the proper discharge of its financial, legal and reporting obligations. The Company's records must be honest, accurate and complete and must fairly represent the facts. The knowing or deliberate falsification of any documents may be the

basis for immediate discharge and may subject an Employee to civil and criminal sanctions as well.

All account books, budgets, project evaluations, expense accounts and other papers utilized in maintaining records of the Company's business must accurately reflect the matters to which they relate. Without limiting the foregoing, all public communications and filings (including any reports and documents filed with the Securities and Exchange Commission), should be full, fair, honest, timely, accurate and understandable. All assets of the Company must be carefully and properly accounted for. No payment of funds of the Company shall be approved or made with the understanding that any part of the funds will be used in a manner contrary to this principle.

Dishonest reporting of information to organizations and people inside or outside the Company, including false or artificial entries in books and records, is strictly prohibited. It could lead to civil or criminal liability for you and the Company. This includes not only reporting information inaccurately but also organizing it in a way that is intended to mislead or misinform those who receive it. No undisclosed or unrecorded funds or assets shall be established for any purpose. In a case where the Company permits petty cash funds to exist, such funds must be administered pursuant to the Company's system of internal controls.

The Company's independent registered public accountants shall be given access to all information necessary for them to conduct audits properly. Employees must not, and must not direct others to, take any action to fraudulently influence, coerce, manipulate or mislead any public or independent registered 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 will be deemed 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 influence, if successful, would result in rendering financial statements materially misleading.

Business, tax, financial reporting and legal considerations require the orderly retention of Company records. For this purpose the Company has in place a Policy Statement on Record Retention which applies to electronic as well as paper records. All Employees must comply with this Policy, and Employees are urged to familiarize themselves with the Policy. The retention periods set forth in the Policy govern all Company records unless a directive has been issued by the Company advising that the purging of all or certain categories of documents has been sus-

pended (for example, because of an imminent, threatened or pending government or regulatory investigation or proceeding, a pending civil litigation or proceeding, a subpoena or the like) until further notice. If any Employee believes that any records should be preserved beyond the prescribed period, for any reason (for example, because of knowledge of an imminent or threatened investigation or proceeding), advice should be sought immediately from the Chief Financial Officer and/or Director of Compliance.

If and to the extent the Company becomes subject to the reporting requirements under the Securities Exchange Act of 1934 (the "Exchange Act"), the Company will follow the accepted accounting rules and controls as set forth by the Securities and Exchange Commission and the Financial Accounting Standards Board and the accounting practices prescribed or permitted by regulatory authorities as well as the applicable local accounting rules and principles, and the foregoing shall be deemed to include any additional requirements to which the Company thereby becomes subject.

See the Company's "Policy Statement on Record Retention," which is attached as Appendix B of this Code.

6. E-MAIL/PC COMMUNICATIONS

All computer hardware and software and other equipment, such as electronic devices, including but not limited to cell phones, personal digital assistants, personal communications devices and tablets provided to Employees by the Company (hereinafter "Equipment"), as well as any information or data transmitted by or stored in such systems or Equipment (including electronic mail), are Company property and should be used primarily for business purposes. Occasional personal e-mails or other communications and occasional personal access to the Company-supplied Internet service are permitted, but the standard of reasonableness should govern. Thus, extensive personal use of the Company-supplied Internet service as well as extensive use of the computer system or other Company Equipment for personal e-mail or other communications is forbidden. For purposes of the Code, "Personal Devices" shall be deemed to include personal devices not owned by the Company to the extent used for Company business. The Company reserves the right to monitor and inspect all electronic media, and all communications received or sent using Equipment, as well as all communications on Personal Devices related to or referencing Company business or which have accessed Company-supplied Internet services. Being mindful of the privacy of our Employees, administration of this policy with regard to Personal Devices shall have the goal of providing the Company with reasonable ability to monitor Company-related communications sent from Personal Devices, without being intrusive on Employees' private information. Employees should not have any expectation of privacy when using Company-supplied Internet services or Equipment unless otherwise required by law. Any surveillance of emails or other forms of communication will be conducted in accordance with local legal and regulatory requirements. Employees should not participate in any online forum where the business of the Company or its customers or suppliers is discussed due to the possibility of violating the Company's confidentiality policy or subjecting the Company to

legal action for defamation. The Company's e-mail system or other Equipment used for Company business may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. It may not be used to create any offensive or disruptive messages, such as messages which contain sexual implications, racial slurs, gender-specific comments or offensive references to one's age, sexual orientation, religious or political beliefs, national origin or disability or in any other way which may involve or lead to a breach of this Code or of any applicable laws or regulations.

See the Company's "Policy Statement on Use of the Company's Computer Network, Including E-Mail Communications," which is attached as Appendix C of this Code.

7. POLITICAL CONTRIBUTIONS AND INVOLVEMENT IN POLITICAL ACTIVITIES

No contributions or expenditures will be made by or on behalf of the Company, directly or indirectly, to political candidates, causes or parties, except with the approval of the Board of Directors and in accordance with applicable law. Employees are encouraged to vote and participate fully in the political process. Employees who participate in partisan political activities must make every effort to ensure that they do not give the impression that they speak or act for the Company. Any Employee's personal political contributions cannot be reimbursed by the Company, directly or indirectly.

When dealing with public officials, Employees must avoid any activity that is, or is likely to be perceived as, illegal or unethical, or that reflects a favoritism not accorded to others. The appearance of impropriety is as damaging to our Company as an actual misdeed. Employees must exercise caution to prevent relationships and dealings with public officials from becoming subject to question.

In the event that the Company or any subsidiary of the Company enters into a contract with any state legislative or executive branches or any state quasi-public agency or submits a bid or holds a valid prequalification certificate issued by a state, the Director of Compliance should be promptly notified. In such event he will provide guidance regarding the prohibitions imposed by the State on state contractors which include prohibitions on contributions to candidates for specific offices and contributions to their political committees, by "principals" of state contractors whose contracts or bids meet certain financial thresholds as well as prohibitions on soliciting contributions from the contractor's employees or subcontractors. The prohibitions cover, among others, members of the Board and officers and employees having managerial or discretionary responsibilities to administer the state contract, as well as spouses and dependent children.

8. 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 the Director of Compliance on all antitrust-sensitive matters. Criminal antitrust violations (which exist in many countries) are punishable by large fines and incarceration. Civil antitrust violations could result in fines on the

Company. Enforcement agencies worldwide may offer amnesty to those who first report criminal violations. Amnesty and/or a significant reduction in fines may also be available to the Company if it cooperates with the relevant anti-trust regulators. Thus, suspected problems should be brought to the attention of the Director of Compliance without delay.

In general, antitrust and anti-competition laws prohibit agreements or actions that may unreasonably restrain trade or reduce competition. Violations include agreements among competitors or others to fix or control prices, rig bids or to allocate territories, markets or customers. Exceptions may exist for lawful joint ventures or regulated activities. Subject to the confirmation by the Director of Compliance after consultation with Company's outside counsel that there exist any permitted exceptions, the Company prohibits Employees from participating in any discussions or other communications, understandings or agreements with, or for the benefit of, a competitor regarding:

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

Industry exchanges of price data or other sensitive information must strictly comply with legal requirements and should not be undertaken without approval of the Director of Compliance. Participation in insurance and reinsurance pools must also strictly comply with legal requirements, particularly in the European Union.

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 in order to lessen competition by, for example, conferring a commercial advantage upon a third party and/or creating a false appearance of legitimate competition within the insurance industry.

9. SECURITIES TRADING

The purchase or sale of securities while possessing material nonpublic information ("inside information") or the disclosure of inside information ("tipping") to others who may trade in such securities is sometimes referred to as "insider trading" and is prohibited by U.S. federal and state securities laws, and which precepts the Company expects all Employees to follow regardless of whether the Company shares are privately held or have been publicly registered. As part of your work, you may have access to material nonpublic information about the Company.

The Company has adopted the "Policy Statement on Insider Trading," which is attached as Appendix E of this Code, to assist it in preventing illegal insider trading(in the event the Company's shares become publicly registered) and to avoid even the appearance of improper conduct on the part of any director or Employee, consultant or contractor of the Company. The Policy Statement on Insider Trading is designed to protect and further the Company's reputation for integrity and ethical conduct. However, the ultimate responsibility for complying with securities laws, adhering to this policy and avoiding improper transactions rests with you. It is imperative that you use your best judgment and that you ask questions where you are uncertain how to handle a particular situation.

If and to the extent the Company becomes subject to reporting requirements under the Securities Exchange Act of 1934 (the "Exchange Act") through a public issuance of Company shares, the following is a summary of the principal additional requirements to which all directors and Employees must adhere relating to the trading of the Company's securities. However, Employees must also be familiar, and comply, with the Company's "Policy Statement on Insider Trading," which is attached as Appendix E of this Code, in its entirety and should consult with the Director of Compliance in the event there are any questions concerning the policy.

A. Trading Restrictions. Trading by an Employee is not permitted if such Employee possesses material nonpublic information. In addition, trading is not permitted during any blackout period, so notified by the Director of Compliance, until that period has been terminated by notice from the Director of Compliance.

B. Additional Restrictions With Respect to Restricted Group Members. To provide assistance in preventing inadvertent violations and avoiding even the appearance of an improper transaction (which could result, for example, where an insider engages in a trade while unaware of a pending major development), the procedures set forth below must be followed by all WHL directors and other Company employees designated from time to time by the Director of Compliance ("restricted group members").

1. *Notification*. Before trading the Company's securities during a Trading Window (as defined below) a restricted group member must provide two business days' prior notice to the Director of Compliance.

2. *Preclearance*. Before trading the Company's securities at any time other than during a Trading Window, a restricted group member must obtain the prior approval of the Director of Compliance.

3. *Blackout Period*. Upon notifying or seeking prior approval from the President and/or the Director of Compliance before trading the Company's securities, a restricted group member will be informed as to whether a blackout period has been imposed.

4. *Filings*. A restricted group member trading in the Company's securities should consult with the President and/or the Director of Compliance or his designee to arrange for the timely preparation of any required filings.

For purposes of the preceding paragraph, "Trading Window" means the period commencing at the opening of trading on the second full trading day following the Company's public release of quarterly or annual financial results and ending on the close of business on the fifteenth day of the third calendar month of that calendar quarter.

C. No Tipping. No Employee who has material nonpublic information relating to the Company may "tip" or disclose such information to others who do not have a legitimate business reason to know such information. In the event any confidential information is disclosed to an outsider, the Company will take such steps as are necessary to preserve the confidentiality of such information, which may include requiring the outsider to agree in writing to comply with the terms of this policy and/or to sign a confidentiality agreement. The Director of Compliance should be notified in the event the disclosure of such information is made in connection with the Company's business activities.

10. ANTI-BRIBERY AND CORRUPTION

The Company will not engage in bribery or corruption in any form (whether it involves private individuals or government officials) and has a zero tolerance approach to violations.

The Company prohibits any Employee, or any person acting on behalf of the Company, from directly or indirectly requesting, accepting, soliciting, agreeing to receive, promising, offering or giving a bribe (which includes facilitation payments, kickbacks or other any other improper payments or financial advantages) to any person.

The Company prohibits any Employee or any associated person acting on behalf of the Company from offering, paying, promising to pay or authorizing the payment of money or anything of value, directly or indirectly, to an officer or employee of a government (including a state-owned commercial entity), legislative, administrative or judicial body, political party, party officials, candidates for political office and officers or employees of public international organizations with the intent or purpose of obtaining, retaining or directing business, a concept which is broadly construed to include seeking any commercial advantage.

All of the Company's activities must be managed in full compliance with the Code and all applicable legal and regulatory anti-bribery and corruption obligations, including the U.S. Foreign Corrupt Practices Act and The UK Bribery Act.

Violations of this prohibition may subject the Company and any involved Employees or agents of the Company to severe civil and/or criminal penalties under the laws of the United States, the United Kingdom and many foreign jurisdictions in which the Company does business. Any known or suspected bribery or corruption problems should be brought to the attention of the Director of Compliance or his/her designee without delay.

11. COPYRIGHTS

Copyright laws protect original creative expression in a number of forms, including written materials, software and the like, and prohibit their unauthorized duplication and distribution. Employees are prohibited from reproducing, distributing or altering copyrighted materials from books, trade journals, computer software, magazines, tapes, disks or videotapes without permission of the copyright owner. Using unlicensed software could constitute copyright infringement. The Company subscribes to a number of trade journals and magazines and Employees must take particular care to avoid copying portions of these materials for distribution to others.

12. POLICY AGAINST DISCRIMINATION AND HARASSMENT

The Company is committed to providing equal employment opportunities to all Employees and prospective Employees in every facet of its operations. All employment-related decisions, including hiring, employee treatment, training, compensation, promotion, transfer, benefits and disciplinary action, are made solely on the basis of the individual's job qualifications and performance, and without regard to race, color, religion, creed, sex, national origin, ancestry, disability, age, genetic information, citizenship status, pregnancy, sexual orientation, marital status, veteran status, membership in the armed services, political affiliation, or any other characteristic protected by law.

It is also the policy of the Company that sexual, ethnic, racial as well as any other form of harassment prohibited by law is unacceptable conduct in the workplace and will not be tolerated. Behavior constituting harassment on any basis prohibited by law will be treated with the utmost seriousness and may result in disciplinary action, including immediate termination of employment. Conduct of this type engaged in by contractors, vendors and clients toward Employees in our workplace will similarly not be tolerated.

No individual who raises a concern regarding a violation of the Company's policies against discrimination or harassment will be penalized or otherwise retaliated against.

See the Company's "Policy Statement Against Discrimination and Harassment," which is attached as Appendix D of this Code.

13. ALCOHOL AND DRUGS

Employees are expected to perform their duties free from the influence of any controlled substance, including alcohol or illegal drugs, which would impair performance or negatively impact the performance of others. .

The possession, use, sale or distribution of illegal drugs in the workplace will not be tolerated.

The Company, in its discretion, reserves the right to randomly test Employees for the use of alcohol or other controlled substances, unless prohibited by prevailing local or state law.

14. PROTECTING OUR ENVIRONMENT

The Company is committed to protecting and improving the environment in all areas of the Company's operations, thereby preserving and enhancing the quality of life of our Employees, customers and neighbors. This commitment is a shared responsibility with all Employees.

15. SAFETY

The Company strives and is committed to providing its Employees with a healthy and safe environment.

The Company is committed to providing the best possible working conditions for its Employees. The place of employment is to be free of recognized hazards that might cause injury or death as well as be in compliance with specific safety and health standards.

All Employees have the responsibility to their fellow Employees and to the Company to carry on their duties in a safe and efficient manner. Employees must report any unsafe conditions and immediately correct any unsafe acts observed or performed.

16. RETENTION OF AGENTS AND REPRESENTATIVES

Agents and representatives cannot be used to circumvent the law or this Code. All agents and representatives should possess the requisite business ethics required by the Company and therefore due care, skill and diligence shall be used when appointing any agent or representative. Any questions in this regard should be directed to the Director of Compliance or his/her designee.

For the avoidance of doubt, for purposes of this Code, employees of Arch Underwriters Ltd. ("AUL") and Arch Underwriters Inc. ("AUI") or their affiliates made available to the Company on a non-exclusive basis pursuant to those certain Services Agreements between the Company and AUL or AUI, respectively (and as may be amended or supplemented from time to time) shall not be deemed to be Employees of the Company and shall instead be deemed to be agents and representatives of the Company when acting on the Company's behalf. All employees of AUL and AUI are required to annually certify to Arch their compliance with the Arch Code of Conduct, which the Company deems to be the conceptual equivalent of this Code.

Non-Employee officers and directors of Watford Insurance Company Europe Ltd. are deemed agents and Representatives of the Company and shall be required to annually certify compliance with this Code to the Director of Compliance.

17. ANTI-BOYCOTT

Laws and regulations implemented by the United States contain a broad range of sanctions directed at U.S. companies (including foreign entities controlled by domestic entities) which participate in boycotts of other countries which are not approved by the United States (for example, the Arab boycott of Israel). Violations of regulations implemented by the U.S. Department of Commerce, including failure to report receipt of boycott-related requests such as requests for information concerning relations with blacklisted companies, can subject violators to substantial civil and criminal penalties. Regulations implemented by the U.S. Department of the Treasury subject taxpayers to loss of tax credits for agreeing to participate in a non-sanctioned boycott. All Employees shall refer any request to participate in any non-sanctioned boycott to the Director of Compliance or his/her designee. The foregoing applies to persons and entities that are subject to U.S. laws.

18. PROHIBITIONS ON FINANCIAL TRANSACTIONS INVOLVING DESIGNATED COUNTRIES, ENTITIES AND PERSONS

Many of the countries in which the Company transacts business, including the United States, the member states of the European Union (including the United Kingdom), Switzerland and Canada, have enacted prohibitions against financial transactions involving designated countries, or persons or entities acting on their behalf. Furthermore, pursuant to United Nations and European Union restrictions, hundreds of countries have imposed asset freezes on various terrorists and terrorist organizations. Employees of the Company must be vigilant and comply with all applicable laws and regulations.

Because of the very serious consequences of violating these restrictions — civil and criminal penalties and likely damage to the Company's reputation — Employees of the Company must comply with all applicable laws and regulations. It is essential that Employees "Know Their Customers" and that thorough and frequent checks are made to ensure that transactions involving those customers are not restricted by applicable laws. A first step in finding information on these restrictions may be secured at the following websites:

- United States Treasury Department Office of Foreign Assets Control: http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
- United States Department of Commerce, Bureau of Industry and Security "Lists of Parties of Concern": http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern
- United Nations: http://www.un.org/sc/committees/ (A compendium can be found at http://www.un.org/sc/committees/list_compend.shtml)

- European Union: http://eeas.europa.eu/cfsp/sanctions/index_en.htm
- United Kingdom: http://www.hm-treasury.gov.uk/fin_sanctions_index.htm
- Canada: http://www.international.gc.ca/sanctions/index.aspx?lang=eng
- Switzerland: http://www.seco.admin.ch/themen/00513/00620/index.html?lang=en
- Australia: http://www.dfat.gov.au/un/unsc_sanctions/index.html

19. MONEY LAUNDERING

All Employees must be vigilant in order to protect the Company from being unknowingly swept into a money laundering transaction. Money laundering is a term used to describe the process of integrating proceeds from illegal activities into the legitimate financial system so that the proceeds appear to have originated from a legitimate source. Transactions need not be cash transactions to constitute money laundering and money laundering can involve any movement of funds, cash or otherwise. Many countries, including the United States, Canada, United Kingdom and Bermuda, have adopted statutes which make participation in money laundering a criminal offense and subject the offender to harsh penalties.

Fundamental stages of money laundering include the placement or physical disposal of criminal proceeds into the financial system, followed by the creation of layers of transactions designed to obscure the source. Money laundering also includes use of the financial system to further international criminal activity.

Any Employee who knowingly permits illegal conduct or closes his or her eyes to suspicious activity that indicates possible money laundering will not only be subject to discipline by the Company, but may also subject himself or herself and the Company to criminal and civil penalties.

Money laundering issues are complex and you should not attempt to handle them on your own. If you become aware of any questionable circumstances, which could suggest money laundering, or if you have any questions, you must promptly consult the Director of Compliance or his/her designee.

The Company's program of vigilance to combat any attempt to use the Company's facilities to launder money consists mainly of the following key elements:

1. Verification, or "Knowing Your Customer"
2. Maintaining documentation
3. Recognition and reporting of suspicious transactions
4. Training

The Financial Crimes Enforcement Network of the U.S. Department of the Treasury has promulgated regulations requiring that insurance companies that deal in "covered products" adopt anti-money laundering programs. "Covered products", which are those that present significant risk for money laundering, are:

- permanent life insurance policies, other than a group life insurance policy;
- annuity contracts, other than group annuity contracts; and
- any other insurance product with features of cash value or investment.

Other laws and regulations may apply to subsidiaries or branches of the Company located outside the United States, and Employees of those subsidiaries and branches of the Company must comply with any local requirements.

With respect to "covered products" the following steps must be undertaken in the United States:

1. Verification, or "Knowing Your Customer"

Most of the Company's customers are large, established corporations and institutions listed on recognized stock exchanges or subsidiaries of such companies and pose little risk of money laundering because of their financial transparency. For these customers, the preparation of standard account opening and transaction documentation would be sufficient verification, absent questionable circumstances.

In the case of customers less known or not known to the Company at all and companies not quoted on a recognized stock exchange or their subsidiaries, we must be satisfied that the customer is a legitimate entity engaging in a legitimate transaction and verification procedures must be undertaken. For example, steps should be taken to verify the customer's underlying beneficial owners, that is, those who ultimately own or control the customer (for example, those with interests of 5% or more). Individuals who seek to become customers and who are not known to the Company should be personally interviewed regarding the nature and history of their business. Accounts handled by an intermediary may present specific risks, particularly when the beneficial owners are not identified.

2. Maintaining documentation

The Company's policy is to retain for a minimum period of five years all documentation relating to the verification of the identity of the customer, as well as all records relating to each transaction, in readily retrievable form. Such records must be maintained even after the customer relationship has been terminated.

3. Recognition and reporting of suspicious transactions

Once an account is opened, it must be monitored for any signs of money laundering. Suspicions must be reported to the Director of Compliance or his/her designee and you must not disclose this information to the customer. A suspicious transaction would include one that is inconsistent with a customer's known legitimate business or activities, one involving unusual payment methods or one involving early termination with the proceeds directed to a third party.

4. Training

To the extent needed, the Company may also give more specialized training to employees whose duties could expose them to attempted money laundering, such as employees responsible for the opening of new accounts, as well as the training of their superiors.

LIST OF SUBSIDIARIES (FEBRUARY 2017)

Watford Holdings Ltd.[1]

Watford Re Ltd.[1] and its subsidiaries, including:

Watford Insurance Company Europe Limited[2]

Watford Holdings (UK) Limited[3] and its subsidiaries, including:

Watford Holdings (US) Inc.[4]

Watford Services Inc.[5]

Watford Specialty Insurance Company, including subsidiary[4]

Watford Insurance Company[4]

Notes:
[1] Bermuda company
[2] Gibraltar company
[3] UK company
[4] Delaware company
[4] New Jersey company

COMPLIANCE HOTLINE NUMBERS

	Telephone
Outside of the United States:	866-369-2178
Within the United States:	866-369-2178
WTRE@openboard.info	

COMPLIANCE PERSONNEL

	Name	Location	Telephone	Fax	E-Mail
Director of Compliance	Laurence Richardson	Watford Holdings Ltd. Waterloo House, 1st Floor 100 Pitts Bay Road Pembroke HM 08, Bermuda	441-599-9166	441-278-3451	lbr@watfordholdings.com
Corporate Counsel to Watford Holdings Ltd.	Gary Boss, Esq.	Clifford Chance US LLP 31 West 52nd Street New York, NY 10019-6131	212-878-8000	212-878-8375	Gary.Boss@CliffordChance.com
Designees for Subsidiaries					
Watford Re Ltd.	Robert Hawley	Watford Holdings Ltd. Waterloo House, 1st Floor 100 Pitts Bay Road Pembroke HM 08, Bermuda	441-278-3456	441-278-3451	rhawley@watfordre.com
Watford Insurance Company Europe Limited	Laurence Richardson	Watford Holdings Ltd. Waterloo House, 1st Floor 100 Pitts Bay Road Pembroke HM 08, Bermuda	441-599-9166	441-278-3451	lbr@watfordholdings.com
Watford Holdings (US) Inc.*	Eileen Sorabella	Watford Holdings (US) Inc 445 South Street, Morristown, NJ 07962	973-889-6464	TBC	esorabella@archcapservices.com

* Watford Holdings (US) Inc. includes Watford Services Inc.,Watford Specialty Insurance Company and Watford Insurance Company

POLICY STATEMENT ON CONFIDENTIAL INFORMATION

Scope of Policy: The following policy relating to disclosure of confidential information applies to all directors, officers and Employees (collectively, "Representatives") of the Company.

CONFIDENTIAL INFORMATION

A. Purpose of Policy. Serious problems could be caused for the Company and its personnel by the unauthorized disclosure of internal information concerning the Company. In addition to possibly violating the law (particularly if for the purpose of facilitating improper trading in the Company's securities), such disclosure could, among other things, competitively disadvantage the Company or breach a confidence of a client of the Company. The Chief Financial Officer and/or the Director of Compliance may, in their discretion, determine to consult with the Company's outside counsel on any of the matters arising within this Policy Statement.

B. Policy. A Representative must not discuss internal Company matters or developments with anyone outside the Company, except as required in the performance of regular corporate duties, whether or not the information in such Representative's possession is proprietary information concerning the Company. Confidential information should be disclosed only to key personnel and principal outside advisers whose work for the Company requires that they have such information. Finally, Representatives should not discuss Company matters on Internet chat rooms or other on-line services or message boards.

1. Responding to Inquiries. The prohibition on disclosure applies specifically (but not exclusively) to inquiries concerning the Company which may be made by the industry press, financial press, investment analysts or others in the investment community or shareholders. All such communications on behalf of the Company must be channeled through an appropriately designated officer under carefully controlled circumstances. Unless you are expressly authorized to the contrary (see below), if you receive any inquiries of this nature, you must decline comment and refer the inquiries to the Chief Financial Officer or the Director of Compliance.

2. Designated Officials. Only the following Representatives are authorized to respond to such inquiries on behalf of the Company: (i) the Chairman of WHL's Board of Directors, (ii) the Chief Executive Officer, (iii) the Chief Financial Officer, (iv) the Director of Compliance and (v) (as to specific inquiries) persons designated to respond by the Chief Financial Officer or

the Director of Compliance. Any Representative authorized to so respond should, if practicable, consult with the Chief Financial Officer and/or Director of Compliance within a reasonable time before responding to such inquiry and, in all cases, inform the Chief Financial Officer and the Director of Compliance of the inquiry and the nature of the response provided.

3. No Trading Advice. Regardless of the Company's status as a privately-held company, and particularly in the event the Company becomes subject to the reporting requirements under the Securities Exchange Act of 1934 (the "Exchange Act"), all Representatives are discouraged from providing trading advice of any kind concerning the Company to any third party (even when Representatives do not possess material nonpublic information), except that all persons given access to confidential information should be advised (i) of their status as a "Representative" and informed of the Exchange Act's prohibition against trading in the Company's securities and (ii) not to disclose the information further except as absolutely necessary for corporate purposes.

4. Procedure Upon Disclosure. In any instance in which confidential information is disclosed to an outsider, the Company will take such steps as are necessary to preserve the confidentiality of the information, which may include requiring the outsider to agree in writing to comply with the terms of this policy and/or to sign a confidentiality agreement. The Chief Financial Officer and/or Director of Compliance (or his designee) must be consulted if it is contemplated that confidential information will be disclosed to an outsider.

5. Conversations With Investment Analysts. All conversations with investment analysts should be reported to the Chief Financial Officer or the Director of Compliance.

6. Company Releases. The Chief Financial Officer and/or the Director of Compliance should review and clear all company releases for content, accuracy and legal compliance. The Chief Financial Officer and/or the Director of Compliance also should monitor the dissemination of releases to ensure that information is circulating accurately. If a release was incorrectly quoted, the Chief Financial Officer and/or the Director of Compliance may have to recommend that a follow-up release be issued.

7. Speeches and Interviews; Website Postings. The Chief Financial Officer and/or the Director of Compliance should approve, in advance, commitments for speeches or interviews with the press. Copies of speeches to the investment community should be prepared in advance and reviewed

by the Director of Compliance. Postings on any Company website should also be approved by the Director of Compliance.

8. Analysts' Statements. Generally, the Company should not comment on or distribute analysts' statements. However, there may be specific instances where the Company may decide to correct substantially erroneous analysts' reports, provided that any such correction may be authorized only by the Chairman of WHL's Board, the Chief Executive Officer or the Chief Financial Officer.

POLICY STATEMENT ON RECORD RETENTION

1. PURPOSE OF RECORD RETENTION POLICY.

Local business, tax, financial reporting, legal and regulatory considerations dictate the orderly retention of company records to document the activities of Watford Holdings Ltd. and its wholly owned subsidiaries (the "Company"). At the same time, it is impractical to retain all records indefinitely; record storage expenses would be prohibitive and retrieval of particular records would be difficult at best. Accordingly, it is the Company's policy to retain in its files only those records that are likely to be needed in our business operations. The Company has promulgated this policy in order to achieve these goals.

The actual scope of record retention, as well as the actual retention period, will be based on local, legal or regulatory requirements and practices, but in no case will records be destroyed before the recommended retention period or before the period imposed by local, legal or regulatory requirements.

It is suggested that those Company personnel whose responsibilities include the maintenance of the Company's records conduct annual reviews to ensure compliance with this policy or more frequently if appropriate pursuant to any applicable local laws, guidelines or requirements. In particular, the retention of records regarding Company Employees, agents and representatives located in European Union ("EU") Member States may be dictated by local implementation policies established pursuant to EU Data Protection Directives. Your help and cooperation is appreciated.

2. HOW TO USE THE RECORD RETENTION SCHEDULES.

In order to determine the applicable retention period for Company records, refer to the table beginning on page B-4 of this Policy Statement. Choose the relevant Record Category and Record Title that best describes the record and follow the retention period indicated.

In the event that any record falling within the description of one Record Category contains an attachment that falls within the description of another Record Category, the Record Category governing the retention of the attachment will govern the applicable retention period for the record.

If any employee believes that there is any ambiguity or question regarding the applicable Record Category governing the retention period for a record, the Director of Compliance should be consulted for advice.

3. CONFIDENTIAL RECORDS.

Confidential records that have exceeded their retention period are to be shredded or otherwise destroyed.

4. **ELECTRONIC STORAGE.**

Materials maintained in electronic/digital form should be retained for the same period as the equivalent material in printed form. Records may be stored electronically provided they can be obtained/produced easily during the required retention period. Records generated and maintained in Company information systems or equipment (including mainframe and personal computing/e-mail/word processing/storage systems/websites) are to be regularly reviewed to ensure that the record retention policy is being met for electronic information systems. Each Company subsidiary, and, as applicable, each agent or representative performing contractual services for the Company, will have a designated manager or director who will supervise the retention of files and records related to Company business, and will ensure that the Company has ready access to such records.

With regard to the Company website, the Company must have the ability to demonstrate not only what appeared on its website at any particular time, but also to pinpoint precisely when changes were made. Therefore items originating from the Company's website are to be considered "records" and are subject to the same retention requirements as other "paper" records. The applicable retention period will be determined by the type of document appearing on the website. Website-related retention should be accomplished by simply printing the web page, which will automatically display the date on which it was printed.

Employees are required to comply with the Company's "Policy Statement on Use of the Company's Computer Network, Including E-Mail Communications" which is Appendix C to the Code of Conduct, regarding the proper use and maintenance of company-provided computer equipment and information systems, such as e-mail and word processing. These resources are to be used primarily for business purposes. Employees are required to regularly review, but no less frequently than monthly, all incoming and outgoing e-mails to determine whether such records are for non-business purposes. Unnecessary, non-business records should be deleted from laptops, tablets, servers and desktop hard drives (including material on backup tapes and other media) on a regular basis.

5. **FILES PURGING.**

Each Company subsidiary will have a designated manager or director who will supervise the process of purging Company-related files on at least an annual basis. As applicable, each agent or representative performing contractual services for the Company shall annually review Company-related documents in its possession and will recommend to the Director of Compliance (or his designee) which are to be retained and which may be destroyed. **Company documents may only be destroyed by authorized Employees or at their direction, and only in accordance with the record retention policies herein described.** As a result of this process:

(a) records that require retention are to be identified, grouped, labeled, and transferred to a designated on-site or off-site location for appropriate storage;

(b) records that have exceeded their retention period are to be identified and destroyed; and

(c) unnecessary duplicate and multiple copies of records are to be identified and destroyed.

The retention periods set forth herein will govern all Company records unless a directive has been issued by the Company advising that the purging of all or certain categories of documents pursuant to this Policy Statement on Record Retention has been suspended (for example, because of an imminent, threatened or pending government or regulatory investigation or proceeding, a pending civil litigation or proceeding, a subpoena or the like) until further notice. **In such case, no such documents may be purged until a subsequent directive is issued by the Director of Compliance advising that the suspension has been lifted.**

If any Employee believes that any records should be preserved beyond the period specified in this Policy Statement on Record Retention for any reason, including because of knowledge of an imminent, threatened or pending government or regulatory investigation or proceeding, a pending civil litigation or proceeding, a subpoena or the like, the Director of Compliance should be immediately contacted for advice.

6. **OFF-SITE RECORD RETENTION.**

All surplus records or duplicates made or utilized for off-site use, including those on systems such as laptops, home computers, etc., including correspondence, notes, memoranda, drafts, markups, proofs, computer disks, backup tapes, and the like, are subject to the provisions of the Policy Statement on Record Retention and must be maintained accordingly.

Index to Terms Legend for Retention Period

AC	-	After Completion of Job or Contract
AE	-	After Expiration of Term or Effective Period
AS	-	After Settlement or Resolution of Claim/Litigation/Investigation
AT	-	After Termination
CUR	-	Current (only the current version needs to be retained)
P	-	Permanent
P1	-	One permanent archive copy; destroy remaining copies

*** All retention periods are in years unless otherwise specified.**

RECORD CATEGORIES[1]

7. BUSINESS OPERATION RECORDS

Record Title	Retention Period
Applications For Insurance – No Policy Issued	6
Ceding Company Audits	7
Claim Files	AS + 6
Customer Files (Non-Insurance/Reinsurance)	
• Verification of Identity	AC+5
• Transaction Documents	AC+5
Producer Licensing Records	AT + 6
Regulatory	
• Correspondence with Insurance Regulators	6
• Compliance Files	AS + 6
Reinsurance and Retrocession Agreements (Assumed and Ceded)	P
Reinsurance Submissions - No Treaty Bound or Facultative Certificate Issued	3
Underwriting Files	
• Insurance Policy Issued	P
• Reinsurance Treaty Bound/Facultative Certificate Issued	P

[1] If any Employee, agent or representative believes that there is any ambiguity or question regarding the applicable Record Category governing the retention period for any record, the Director of Compliance should be consulted for advice. If local laws or regulations provide for a longer or mandatory shorter retention period, that longer or shorter period will apply.

8. CORPORATE COMMUNICATIONS RECORDS

Record Title	Retention Period
Community Relations	
• News Releases	6
• Special Events	3
Investor Relations	
• Transcripts of Annual Meeting of Shareholders (Including Meeting Handouts, Etc.)	10
• Communications and Reports to Shareholders	P
• Financial Literature Other Than Shareholder Reports	6
• News Releases	6
• SEC Filings	P
• Shareholder List	10
• Published Speeches	10
Marketing Communications	
• Contracts	AT + 6
• Market and Statistical Information	4
• Misc. Memoranda and Correspondence	4
• Photographs	P1
• Product Advertisements	P1
• Product Technical Literature	P1
• Print Shop Plates and Negatives	P1
• Trade Show Files	CUR + 2

9. **FINANCIAL RECORDS**

Record Title	**Retention Period**
Accounts Payable	6 or after tax audit close
Accounts Receivable	
• Accounts Receivable All Items Listing	6 or after tax audit close
• Accounts Receivable - Aged Trial Balance	6
• Reconciliation with General Ledger and Transfer Journal	CUR
• Write-Off Information for Tax Purposes	6 or after tax audit close
• Accounts Receivable Ageings	1
Bank Records	
• Bank Credit and Deposit Slips	6
• Bank Statements	6
• Canceled and Cleared Checks	6
• Check Copies	6
• Bank Reconciliations	6
Audit, Internal (Including Correspondence, Internal Audit Reports and Work Papers)	6
Audit Reports, External	P
Budget	6
Depreciation Schedules	P
Expense Records	6
General Ledger	P
SEC Filings and External Reporting	P
Except:	
• Supporting Documents	6
Stock Records	P
Tax Records	P
Except:	
• General Memoranda and Correspondence	4
• Tax returns	P

9. **FINANCIAL RECORDS (continued)**

Record Title	Retention Period
Acquisitions and Divestitures	
• Acquisition and Divestiture Assessments (Not Completed)	6
• Acquisitions and Divestitures (Completed)	Selectively weed after 6 years
Except:	
• Closing Documents	P
• Annual and Company Reports	6
• Industry Studies	CUR
Corporate Benefits	
• Employee Expense Reports	6
• Benefit Document Files (Including Pension Plan, Trust Agreements and ERISA and Other Statutory Reports)	P
• General Information and Subject Files	Selectively weed after 1 year
• Location Files	Selectively weed after 1 year
Corporate Risk Management	
Property	Term + 6 years
Liability	
• Claims Made and Reported Policies - No Claims	6
• Claims Made and Reported - with Claims	AS + 6 years
• Occurrence Policy	P
Treasurer Files	
• Bank Files (Including Correspondence and Account Analyses)	Selectively weed after 3 years
• Board Meetings and Materials	4
• Loan Agreements (Including Letters of Credit, Lines of Credit, Notes, Commercial Paper, Etc.)	AT + 6
• Management Studies	3
• Miscellaneous Subject Files	Selectively weed after 3 years
• Pension Files	P
• SEC Filings	P
Segment Income Statements	
• Monthly	CUR
• Annual	3

9. **FINANCIAL RECORDS (continued)**

Record Title	**Retention Period**
Reports to Directors	4
Internal Management Reports	4
Capital Expenditure Authorization	3
Capital Expenditure Reports	P
Capital Log Books	3
Regulatory	
• Correspondence with Insurance Regulators	6
• Statutory Audit Reports	P

10. **GENERAL CORRESPONDENCE, MEMORANDA, DIARIES, PLANNERS, NOTES, DRAFTS AND PROOFS**[2]

Record Title	**Retention Period**
General Correspondence (Including E-Mail)	4 years or until no longer needed
General Memoranda (Including E-Mail)	4 years or until no longer needed
Diaries (Including Any Personal Diaries Containing Company Information)	1
Planners (Including Any Personal Planners Containing Company Information)	1
Notes, Drafts and Proofs	The earlier of (a) until no longer needed or (b) until incorporated into a final work product such as a letter, a memorandum, a report, a public filing, a press release, a communication to shareholders or employees, tax filings, etc.
Voice Messages	Retain only as needed; do not retain thereafter

2 In the event that record falling within this general Record Category also falls within any more specific Record Category, the record retention period dictated by such other specific Record Category shall be applicable. If any Employee believes that there is any ambiguity or question regarding the applicable Record Category governing the retention period for any record, the Director of Compliance should be consulted for advice.

11. HUMAN RESOURCES RECORDS[3]

Record Title	Retention Period
Payroll	
• Payroll Records	6 or later after tax audit close
Except:	
• Payroll Earnings Records	P
• Payroll Registers, Ledgers and Journals	P
• Time Records (Including Absence Reports)	6
Personnel Records	
• Present Employees	Term of Employment
• Former Employees:	
All Personnel Records to be Discarded	
Except:	
• Application and Resume; Job History	P
• Computerized Employee History File	P
• Documents Signed by Employee	P
• Medical and Health Records	P
• Performance Reviews	P
• Safety Training Files	P
• Salary Increase Forms	P
• Relocation Expenses	P
• Separation Form or Agreement	P
• Unemployment Compensation Forms	P
Medical Benefits	
• Accident Reports	P
• Benefit Claims	18 months after paid out
Regulatory Returns i.e., CURE, EEOC	P
Records of Individuals Not Hired	3
General Memoranda and Correspondence	4
Job Descriptions	CUR
Evaluations	4
Policies and Handbooks	CUR

[3] With respect to Employees that are citizens of an EU member state, local implementation policies established pursuant to EU Data Protection Directives may require shorter or longer retention periods for human resources records. The Director of Compliance should be consulted for current local rules regarding human resource records in EU Member States. In the absence of any such advice, the retention periods included in this Policy Statement on Record Retention will apply.

12. INFORMATION TECHNOLOGY RECORDS

Record Title	Retention Period
Computer Program Listings and Systems Documentation	CUR
Computer Operations Reports	CUR
Correspondence, Subject Files and Reference Files	Selectively weed after 1 year
System Tape Backups	See policies applicable to particular records
System Documentation Including: • System Implementation Documentation • Change of Control Documentation • Acceptance Testing • Feasibility Studies • Data Conversion Testing	Life of system + 2 years

13. **LEGAL RECORDS**

Record Title	**Retention Period**
Board and Shareholder Minutes	P
Bylaws/Charters/Constitution/Incorporation Records	P
Building Plans	Life of building
Communications and Reports to Shareholders	P
Contracts	AT + 6
Charitable Contributions	6
Correspondence and Memoranda	4
Dividend Register	P
Financial Statements and Reports (Including Budgets)	P
Management Studies and Board Presentations	4
SEC Filings	P
Stockholder Meeting	P
Except:	
• Shareholder List	10
• Proxy	2
Stock Certificates (Canceled)	10
General Records	
• Contracts	AT + 6
• Correspondence and Memoranda	4
• Deeds/Abstracts/Titles	P
• Easements/Rights of Way/Water Rights/Zoning	P
• Lawsuits/Claims	AS + 6
• Leases (Plant and Equipment)	Life of property or until transferred
• Mortgages	Life of property or until transferred
• Stock Records	P
• Legal Opinions	P
• Shareholder Lists	P

13. **LEGAL RECORDS (continued)**

Record Title	Retention Period
Trademarks or Service Marks	
• Original Grant of the Trademark or Service Mark	AE or AT+6
• One Copy of Application as Filed, Oath or Declaration, Assignment, Each Written Communication Between Applicant and the U.S. or Foreign Trademark Office in Connection with Prosecution of the Application, Samples of the Mark, Protest Letters and Other Correspondence with Third Parties Concerning the Enforcement of the Mark, Search Requests and Reports, Agreements with Third Parties Relating to the Mark	AE or AT+6
• One Copy of Each Document Evidencing First Use	AE or AT + 6
• Formal Written Opinions Relating to Registrability and Availability for Use	AE or AT + 6
• Drafts	Retain only as needed until document is finalized; do not retain thereafter
Acquisition and Divestiture Assessments (Not Completed)	6
Acquisitions and Divestitures (Completed)	Selectively weed after 6 years
Except:	
• Closing Documents	P
Annual and Company Reports	6
Competitive Business Assessments and Evaluations	CUR
General Market Data and Product Information	CUR
Journals and Publications	CUR
Reports on Products and Operations	1
Reports on Resources	P
Budgets	6

14. **PURCHASING RECORDS**

Record Title	**Retention Period**
Awarded Contracts (Including Purchase Order Agreements, Invoices, Service Agreements, Acknowledgments and Acceptances)	AT + 6
Bid Documents, Quotations, Award Correspondence and Purchase Requisitions (Whether in Connection with Awarded Contracts or Unsuccessful Bids)	4
Except:	
• Any Such Documents Referenced in Awarded Contract and/or Purchase Order	AT + 6
Certificates of Insurance	P
Miscellaneous Correspondence and Memoranda	4
Property Appraisal Reports	CUR; discard when property transferred

POLICY STATEMENT ON USE OF THE COMPANY'S COMPUTER NETWORK, INCLUDING E-MAIL COMMUNICATIONS

Watford Holdings Ltd. and its wholly-owned subsidiaries (the "Company") relies on its computer network and systems equipment, such as electronic devices, including but not limited to cell phones, personal digital assistants, personal communications devices and tablets (hereinafter "Equipment"), to conduct its business. To ensure that the network and the Company's Equipment are used responsibly and lawfully by all users, including employees, independent contractors, representatives and agents ("Users"), the Company has adopted this Policy Statement. All Users of the Company's computer network and Equipment are required to agree to comply with the terms of this Policy Statement.

The Policy Statement may be amended from time to time, at the Company's discretion, and Users will be provided with copies of any such amendments.

Violations of this Policy Statement may result in disciplinary action. As to employees, such disciplinary action could include suspension or termination. In the case of independent contractors, representatives and agents, violation could result in the Company's severing the relationship. In all cases, violations could result in civil and/or criminal liability.

The Company's Policy Statement is as follows:

1. The Company's computer network and systems and Equipment are to assist Users in the performance of their jobs and should be used primarily for business purposes and not for personal use. Occasional personal e-mails or other communications and occasional personal Internet access are permitted, but the standard of reasonableness should govern. Thus, extensive personal use of the Internet as well as extensive use of the computer system or Equipment for personal e-mail or communications are forbidden. Users should not have an expectation of privacy and (to the extent permitted by applicable local law) Users expressly waive any right of privacy and agree that the Company has the right, but not the duty, to monitor and review, through human or automated means, all electronic communications and all Equipment belonging to the Company or brought onto Company premises, including all aspects of its computer system, including, but not limited to, monitoring sites visited by Users on the Internet, reviewing material downloaded or uploaded by Users and reviewing e-mail or other communications sent to and received by Users. Such monitoring or review shall be conducted in accordance with local legal and regulatory requirements. Any Company information or data transmitted via or stored in the Company's systems, including all messages composed, sent, received or stored in the e-mail or other communications systems, are and remain the property of the Company. Information or data relating to Company business transmitted via or stored in a User's own PC or Equipment are considered to be the property of the Company.

2. Users must use the same care in drafting e-mail and other electronic communications as would be used in drafting any other written communication. These materials are treated for record retention purposes, and for discovery in litigations, just like hard copies of documents. Too often Users mistakenly view electronic communications as an informal method of communicating, like talking on a telephone. Remember when you are drafting electronic communications that you are creating something that will likely be seen by many persons and could be discoverable in a litigation. Use clear, precise language. Do not use language that can easily be misinterpreted.

3. The use of e-mail or other communications within the Company and on the Internet requires the highest level of confidentiality. The confidentiality of electronic communications should not be assumed. Since there can be no assurance that both e-mail text and attachments and other electronic communications sent within the Company and on the Internet will not be seen, accessed or intercepted by unauthorized parties, code names should be utilized in an e-mail correspondence relating to confidential transactions to the maximum extent possible. Dissemination of e-mail login names, passwords or other personal information over e-mail or other electronic equipment is prohibited as it affects the security of the Company's internal computer and other systems and Equipment. In addition, the e-mail and other communications systems shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

   Images and contents of websites on the Internet may be protected by copyright. While Users may print the contents of a website, some websites may prohibit use of the images or contents. In such cases these images and contents should not be used in materials prepared for the Company without authorization from the website owner.

4. Users shall not use a password, access a file, or retrieve any stored information, unless authorized to do so. Users should not attempt to gain access to another employee's messages or communications without the permission of the latter. Each computer password must be made available to the Company's Director of Compliance or his/her designee upon request.

5. Material that is fraudulent, harassing, racist, sexually explicit, profane, obscene, offensive, intimidating, defamatory or otherwise unlawful or inappropriate may not be sent by e-mail or other form of electronic communication, downloaded from the Internet, or displayed or stored in the Company's computer system or Equipment. The Company is not responsible for material viewed or downloaded by Users from the Internet. Users encountering or receiving this kind of material should immediately report the incident to the Director of Compliance (or his/her designee).

6. Users may not deliberately waste the resources of the Company's computer network and systems infrastructure or Equipment. Users should not send mass mailings or chain

letters, or communications or spend excessive amounts of time on the Internet or otherwise create unnecessary network traffic.

7. Users should not use non-Company purchased software or hardware on Equipment used for Company business unless prior written permission has been secured from the Director of Compliance (or his/her designee) or unless the group has adopted a policy expressly authorizing such usage. Software utilized by the Company may be subject to use restrictions, such as restrictions which prohibit transfer of copies over the Internet, or which prohibit making copies, or which provide that the software may be used only on hardware owned or approved by the Company. Users must comply with any such restrictions so as to avoid copyright violations. Users should address questions regarding such restrictions to their Director of Compliance (or his/her designee).

8. Users should not participate in any electronic forum which discusses the Company or persons or entities with which the Company does business or about which the Company possesses confidential information.

9. With respect to confidential information:

    a. All Users must use password protected screen savers or should log off their computers when they leave their desks.

    b. All confidential information transferred to tablets or other electronic portable media must be locked at night, along with confidential papers, when appropriate, in a secure file cabinet.

    c. All access to confidential information stored on the file server or central computer or Equipment must have password protection or be stored on file share directory with restricted access.

    d. All electronic records should be saved to the appropriate drives if the records relate to the Company's business. Any e-mails which do not relate to Company business should be deleted on a regular basis. The Company's Record Retention Policy governs the destruction of records. However, destruction may be prohibited in the event that a directive has been issued by the Company advising that its Record Retention Policy has been suspended (for example, because of the threat of or commencement of an investigation involving the Company or because of the threat of or filing of a litigation).

    e. Avoid wide circulation of confidential messages or communications. Messages to which the attorney-client privilege may attach should bear an "Attorney Client Privilege and Attorney Work Product" legend. Circulation should be limited to avoid a waiver of the privilege.

10. Users must safeguard their passwords for access to the computer network or Equipment. Users should not adopt passwords which are based on personal information that can be easily guessed. Passwords should not be given to or used by others. Passwords should be changed frequently.

11. Each User is responsible for taking reasonable precautions to ensure that the User's use of the computer network or Equipment does not introduce a virus. Files obtained from outside the Company, files downloaded from the Internet and files attached to e-mails must be scanned with, or will otherwise be subject to, Company-approved virus-checking software. Anti-virus software should not be disabled by end users unless specifically authorized by IT Management.

12. All e-mails or other electronic communications sent outside the Company should include the following legend:

> "The information contained in this e-mail message may be privileged and confidential information and is intended only for the use of the individual and/or entity identified in the alias address of this message. If the reader of this message is not the intended recipient, or an employee or agent responsible to deliver it to the intended recipient, you are hereby requested not to distribute or copy this communication. If you have received this communication in error, please notify us immediately by telephone or return e-mail and delete the original message from your system."

13. In the event that Equipment is lost or stolen, employees must immediately upon becoming aware of such loss or theft report such event to the Company. The Company will attempt to wipe the Equipment of Company information or otherwise take appropriate steps under the circumstances. Users understand that such action may result in the loss of some or all of the information or data stored on the Equipment.

POLICY STATEMENT AGAINST DISCRIMINATION AND HARASSMENT

Policy Against Discrimination

Watford Holdings Ltd. and its wholly-owned subsidiaries (the "Company") are committed to providing equal employment opportunities to all Employees and prospective employees in every facet of their operations. All employment-related decisions, including hiring, Employee treatment, training, compensation, promotion, transfer, benefits and disciplinary action, are made solely on the basis of the individual's job qualifications and performance, and without regard to race, color, religion, creed, sex, national origin, ancestry, disability, age, genetic information, citizenship status, pregnancy, sexual orientation, marital status, veteran status, membership in the armed services, political affiliation, or any other characteristic protected by law.

Policy Against Harassment

It is also the policy of the Company that sexual, ethnic, racial as well as any other form of harassment prohibited by law is unacceptable conduct in the workplace and will not be tolerated. Behavior constituting harassment on any basis prohibited by law will be treated with the utmost seriousness and may result in disciplinary action, including immediate termination of employment. Conduct of this type engaged in by contractors, vendors and clients toward the Company's Employees in our workplace will similarly not be tolerated.

Examples of prohibited conduct include:

- verbal conduct such as racial or sexual epithets, derogatory statements and slurs;
- physical conduct such as improper touching or assault; and
- visual harassment such as racially or sexually explicit or derogatory posters, cartoons or drawings and obscene gestures.

Sexual harassment will not be tolerated in our workplace. Unwelcome sexual advances, requests for sexual favors, and other verbal or physical harassment constitute harassment on account of one's sex when:

(i) submission to or rejection of the conduct is made, either explicitly or implicitly, a term or condition of employment, compensation or advancement, or otherwise forms the basis for employment decisions affecting the individual; or

(ii) the conduct has the purpose or effect of creating an intimidating, hostile or offensive working environment.

No manager or Employee shall threaten or insinuate that an Employee's submission to or rejection of sexual advances will in any way influence any personnel decision involving that employee.

Policy Against Retaliation

No individual who raises a concern regarding a violation of the Company's policies against discrimination or harassment will be penalized or otherwise retaliated against.

Complaint Procedure

Employees who believe they have been subjected to discrimination, harassment or retaliation in violation of the foregoing policies should immediately report their concerns to the appropriate person at the Company. Generally, the first person an Employee speaks to should be the Employee's supervisor or manager. If an Employee does not feel comfortable speaking to his or her supervisor or manager (because, for example, he or she believes that the supervisor or manager is part of the problem), or if he or she is unhappy with the supervisor's or manager's resolution of the matter, he or she should take the issue to the Director of Compliance or the Human Resources Director. If any such concern or issue is reported to a supervisor, manager or Director of Compliance, the supervisor, manager or Director of Compliance should inform the Human Resources Director of the concern or issue.

This complaint procedure also applies to former Employees who believe they were subjected to a violation of our policies against discrimination and harassment during their employment.

All employment-related issues raised in connection with the foregoing procedure are to be handled confidentially to the extent reasonably practicable under the circumstances. Some disclosure may be necessary in order to conduct an appropriate investigation. All supervisors, managers and other Employees are specifically prohibited from taking any retaliatory action against an Employee or former Employee who has raised a complaint pursuant to the above procedure.

POLICY STATEMENT ON
INSIDER TRADING

Scope of Policy: If and to the extent Watford Holdings Ltd. ("WHL") becomes subject to the reporting requirements under the Securities Exchange Act of 1934 (the "Exchange Act"), the following policy relating to trading of securities of WHL and its subsidiaries (collectively, the "Company") shall apply to all directors, officers and Employees (collectively, "Insiders") of the Company. Because these same conceptual restrictions and prohibitions are applicable to privately-held shares as well as publicly-issued shares, during the time that the Company remains privately held, the processes procedures and prohibitions in applicable portions of this policy shall apply to all directors, officers and Employees of the Company, and they should consider themselves "Insiders" for this purpose even though such term is more commonly related to actions involving publicly-issued shares.

II. INSIDER TRADING

A. Purpose of Policy. The purchase or sale of securities while possessing material nonpublic ("inside") information relating to the issuer of such securities is prohibited by federal and state securities laws. In addition, such laws prohibit the selective disclosure of such information to others who may trade. Violation of these provisions may result in civil and criminal penalties, as well as termination of employment. In the course of performing their duties, Insiders may have access to material nonpublic information about the Company or about the Company's business (including information about other companies with which the Company does or may do business). The Company has adopted this policy (i) to comply with securities laws governing (A) trading in the Company's securities; (B) the receipt and use of inside information; and (C) tipping or disclosing inside information; and (ii) to avoid even the appearance of improper conduct on the part of any Insider. Transactions that may be necessary or justifiable for independent reasons (such as the need to raise money for an emergency expenditure) are no exception. Even the appearance of an improper transaction must be avoided to preserve the Company's reputation for adhering to the highest standards of conduct.

B. Policy. No Insider who has material nonpublic information relating to the Company may (i) buy or sell securities of the Company, directly or indirectly, (ii) engage in any other action to take personal advantage of that information or (iii) "tip" or disclose such information to others who do not have a legitimate business reason relating to the Company to know such information, including, without limitation, any family member, friend, casual acquaintance or anyone acting on his or her behalf, as well as analysts, individual investors, and members of the

investment community and news media. This policy also applies to information obtained in the course of employment relating to any other company. On occasion, it may be necessary to disclose material nonpublic information regarding the Company to persons outside the Company for legitimate business reasons. In such circumstances, the Insider must comply with the "Procedure Upon Disclosure" on page A-7 of this policy.

1. Definition of "Material Nonpublic Information".

(a) "*Material Information*". Information concerning the Company, whether positive or negative, is "material" if it would be expected to affect the voting decisions or investment decisions (*i.e.,* whether to buy, sell or hold the Company's securities) of a reasonable shareholder or investor, or if the disclosure of the information could reasonably be expected to significantly alter the total mix of the information in the marketplace about the Company. In simple terms, material information is any type of information which could reasonably be expected to affect the price of the Company's securities. While it is not possible to identify all information that could be deemed "material," the following are examples of types of information that ordinarily would be considered material:

- financial performance, especially quarterly and year-end earnings, and significant changes in financial performance or liquidity
- projections and strategic plans
- potential mergers and acquisitions or the sale of Company assets or subsidiaries
- significant change in capital investment plans
- significant change in reserve policy
- new major insurance or reinsurance contracts or investments
- stock splits, public or private securities/debt offerings, or changes in dividend policies or amounts
- significant changes in senior management

- significant labor disputes or negotiations
- actual or threatened major litigation, or the resolution of such litigation

(b) "*Nonpublic Information*". Material information is "nonpublic" if it has not been widely disseminated to the public, such as through major newswire services, national news services and financial news services or filing containing such information with the Securities and Exchange Commission. 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. For the purposes of this policy, information will be considered public (*i.e.,* no longer "nonpublic") at the opening of trading on the second full trading day following the Company's public release of the information. In determining whether information is nonpublic, please note that:

(1) information received during the course of employment concerning the Company or another company in circumstances indicating that it is not yet in general circulation should be considered nonpublic;

(2) all information that Insiders learn about the Company or its business plans in connection with their employment is potentially "inside" information until publicly disclosed or made available by the Company; and

(3) all such information should be treated as confidential and proprietary to the Company.

2. Securities Covered. The securities to which this policy relates include not only WHL's common shares and preferred shares, but also any publicly traded equity or debt securities of WHL as well as any derivative securities such as options, puts and calls and any other security that relates to, or derives its value by reference to, any securities issued by WHL.

3. No Trading in Derivatives, Short Sales or Purchases on Margin. Insiders shall not engage in the following activities with respect to Company securities:

(1) Short sales;

(2) Purchases on margin; or

(3) Buying or selling put options or call options.

Transactions described in items (2) and (3) above may be conducted with the prior approval of the Director of Compliance.

Securities held in a margin account or pledged as collateral for a loan may be sold without the Insider's consent if the Insider fails to meet a margin call or by the lender in foreclosure if the Insider defaults on a loan. A margin or foreclosure sale that occurs when the Insider is aware of material nonpublic information may, under some circumstances, result in unlawful insider trading. Because of this danger, Insiders should exercise caution in holding Company securities in a margin account or pledging Company securities as collateral for a loan.

4. General. Remember, if a person's securities transactions become the subject of scrutiny, they will be viewed after-the-fact with the benefit of hindsight, and hindsight may indicate that an event was (and should have been viewed as) "material." As a result, before engaging in any transaction each person should carefully consider how regulators and others might view his or her transactions in hindsight. You may always consult with the Director of Compliance prior to engaging in any transaction relating to securities of WHL.

5. Blackout Period. The Director of Compliance may designate a blackout period during which no Insider may trade Company securities without the prior approval of the Director of Compliance until notified by the Director of Compliance that the blackout period has been terminated. Insiders may not disclose to any outside third party that a blackout period has been designated.

6. Additional Restrictions With Respect to Restricted Group Members. To provide assistance in preventing inadvertent violations and avoiding even the appearance of an improper transaction (which could result, for example, where an Insider engages in a trade while unaware of a pending major development), the procedure set forth below must be followed by all WHL directors and other Company employees designated from time to time by the Director of Compliance ("restricted group members"). Restricted group members not in possession of material nonpublic information may trade in Company securities without the prior approval of the Director of Compliance only during the period commencing at the

opening of trading on the second full trading day following the Company's public release (including, for private-placements shares, the investor letter) of quarterly or annual financial results and ending on the close of business on the fiteenth day of the third calendar month of that calendar quarter, provided that restricted group members give two business days' notice to the Director of Compliance. Before trading securities at any other time, including during any "blackout period" (described above) designated by the Director of Compliance, a restricted group member must obtain the prior approval of the Director of Compliance.

Each restricted group member should also pre-clear with the Director of Compliance transactions in the Company's securities by the following persons because the transactions by themselves may be attributed to such restricted group member:

(1) any member of such restricted group member's household;

(2) any trust or estate in which such restricted group member or a household member is a settlor, beneficiary, trustee, executor or the like;

(3) any partnership in which such restricted group member or a household member is a general partner;

(4) any corporation in which such restricted group member or any household members either singly or together own a controlling interest; or

(5) any trust, corporation, charitable organization or other firm, entity or group where such restricted group member or a household member has or shares with others the power to decide whether to buy, sell or hold the Company's securities.

Restricted group members may have certain filing requirements in connection with their purchase or sale of Company securities. Therefore, restricted group members transferring Company securities should consult with the Director of Compliance to arrange for the preparation, in a timely manner, of any required regulatory filings, including a Form 4 or Form 5 and, if a sale of securities is involved, a Form 144, if applicable.

7. Employee Benefit Plans.

(a) *Employee Share Purchase Plan*. The trading prohibitions and restrictions set forth in this policy do not apply to periodic contributions by the Company or employees to employee benefit plans (*e.g.,* pension or 401(k) plans or share purchase plans) which are used to purchase Company securities pursuant to the employees' advance instructions. However, no Insiders may alter their instructions regarding the purchase or sale of Company securities in such plans while in the possession of material nonpublic information. Prior to altering their instructions, Insiders should notify the Director of Compliance.

(b) *Stock Option Plan*. The trading prohibitions and restrictions of this policy apply to all sales of securities acquired through the exercise of stock options granted by the Company, but not to the acquisition of securities through such exercise.

8. Rule 10b5-1 Trading Arrangements. Written trading arrangements that comply with Rule 10b5-1 under the Securities Exchange Act of 1934 ("Rule 10b5-1 Plans") are permitted under this policy. The trading prohibitions and restrictions of this policy apply to the establishment of any Rule 10b5-1 Plans (*e.g.,* restricted group members must give two business days' notice to the Director of Compliance or his designee) but such trading prohibitions and restrictions do not apply to actual transactions effected pursuant to a Rule 10b5-1 Plan. However, no restricted group member may amend or terminate their Rule 10b5-1 Plans without obtaining the prior approval of the Director of Compliance or his designee.

9. Priority of Statutory or Regulatory Trading Restrictions. The trading prohibitions set forth in this policy will be superseded by any greater prohibitions or restrictions prescribed by federal or state securities laws and regulations (*e.g.,* short-swing trading by Insiders under the Securities Exchange Act of 1934 or restrictions on the sale of securities subject to Rule 144 under the Securities Act of 1933) or any greater regulatory and/or statutory prohibitions or restrictions prescribed by any competent authority in a relevant jurisdiction. Any Insider who is uncertain whether other prohibitions or restrictions apply should consult the Director of Compliance or his or her own legal counsel.

CODE OF BUSINESS CONDUCT
ACKNOWLEDGMENT AND CERTIFICATE OF COMPLIANCE

I hereby certify that I have received, read and understand the Code of Business Conduct, including, without limitation, the Policy Statements attached thereto and an integral part thereof, of Watford Holdings Ltd. and its subsidiaries, and agree to its terms and further agree that it is my responsibility to comply with all policies, guidelines and obligations contained therein.

I acknowledge and agree that this Code does not constitute an employment contract, nor a guarantee of continued employment with Watford Holdings Ltd. or any of its subsidiaries. I understand that employees who violate the Code of Business Conduct may be subjected to disciplinary action, including possible termination of employment.

Signature: _____

Print Name: _____

Title/Position: _____

Date: _____

Return this certification no later than two weeks after receipt to your Group Compliance Officer or his/her designee for inclusion as part of your personnel file.

If there is any uncertainty as to the applicability of any principle or policy to a particular situation or the propriety of any contemplated course of action, the Director of Compliance or your Group Compliance Officer (or their designees) should be contacted for assistance and guidance. You may also take advantage of the Compliance Hotline which has been established by the Company.

Contact information for the Director of Compliance and the Group Compliance Officers and the Compliance Hotline telephone numbers appear in Schedule II attached to the Code.