

CODE OF BUSINESS CONDUCT AND ETHICS

Introduction

Crosshair Exploration & Mining Corp. (the “Company”) requires high standards of professional and ethical conduct from its directors, officers and employees (collectively “Company Personnel”). Our reputation with our shareholders, business partners, prospective investors and other stakeholders for honesty and integrity is key to the success of our business. Company Personnel will not be permitted to achieve results through violations of laws or regulations, or through unscrupulous dealings.

This Code of Business Conduct and Ethics (the “Code”) was adopted by the Board of Directors and sets forth the basic principles to guide all Company Personnel. We intend that the Company’s business practices will be compatible with the economic and social priorities of each location in which we operate. Although customs vary by country and standards of ethics may vary in different business environments, honesty and integrity must always characterize our business activity. If a law conflicts with a policy in this Code, you must comply with the law; however, if a local custom or policy conflicts with this Code, you must comply with the Code. If you have any questions about how to handle these situations, you should consult with your supervisor to resolve any conflicts.

This Code reflects our commitment to a culture of honesty, integrity, respect and accountability and outlines the basic principles and policies with which all Company Personnel are expected to comply. Please read this Code carefully.

In addition to following this Code in all aspects of your business activities, you are expected to seek guidance in any case where there is a question about compliance with both the letter and the spirit of our policies and applicable laws. This Code covers a wide range of business practices and procedures. It does not cover every issue that may arise, but it sets out basic principles to guide all Company Personnel of the Company. This Code does not supersede the specific policies and procedures that are covered in the Company’s operating manuals or in separate specific policy statements.

Your cooperation is necessary to the continued success of our business and the cultivation and maintenance of our reputation as a good corporate citizen.

Enforcement of this Code

Those who violate the standards set forth in this Code will be subject to disciplinary action up to and including dismissal. If you are in a situation that you believe may violate or lead to a violation of this Code, follow the guidelines described under the heading “Compliance Procedures” set out below.

Your cooperation is necessary to the continued success of our business and the cultivation and maintenance of our reputation as a good corporate citizen.

Compliance with Laws, Rules and Regulations

Compliance with the letter and spirit of all laws, rules and regulations applicable to our business is critical to our reputation and continued success. All Company Personnel must respect and obey the laws of the cities, provinces, states and countries in which we operate and the rules and regulations of any stock exchanges upon which the Company's securities are traded, and avoid even the appearance of impropriety. Not all Company Personnel are expected to know the details of these laws, but it is important to know enough to determine when to seek advice from supervisors, managers or other appropriate personnel. The Company may hold information and training sessions to promote compliance with laws, rules and regulations, including insider trading laws.

Conflicts of Interest

A conflict of interest occurs when an individual's private interest interferes, or appears to interfere, in any way with the interests of the Company. A conflict situation can arise when an officer, director or employee takes actions or has interests that may make it difficult to perform his or her work for the Company objectively and effectively. Conflicts of interest also arise when an officer, director, employee, or a member of his or her family, receives improper personal benefits as a result of his or her position in the Company. Loans to, or guarantees of obligations of, such persons are likely to pose conflicts of interest, as are transactions of any kind between the Company and any other organization in which you or any member of your family have an interest.

Activities that could give rise to conflicts of interest are prohibited unless specifically approved by the Board of Directors or the Audit Committee. It is not always easy to determine whether a conflict of interest exists, so any potential conflicts of interests should be reported immediately to your supervisor or the Company's Corporate Secretary.

Public Disclosure

Reports and documents that the Company files with any Canadian securities commission, the U.S. Securities and Exchange Commission or other regulatory authority, or releases to the public shall contain full, fair, accurate, timely and understandable information. The chief executive officer and chief financial officer shall review and approve all public disclosures including but not limited to the annual reports, certify and file them with the appropriate regulatory authorities.

Corporate Opportunities

Company Personnel are prohibited from taking for themselves personally opportunities that arise through the use of corporate property, information or position and from using corporate property, information or position for personal gain. Company Personnel are also prohibited from competing with the Company directly or indirectly. Company Personnel owe a duty to the Company to advance the legitimate interests of the Company when the opportunity to do so arises.

Confidentiality

Company Personnel must maintain the confidentiality of information entrusted to them by the Company or that otherwise comes into their possession in the course of their employment, except when disclosure is authorized or legally mandated. Company Personnel may be required to execute a standard form confidentiality agreement upon starting employment or from time to time during the course of employment. The obligation to preserve confidential information continues even after you leave the Company.

Confidential information includes all non-public information that may be of use to competitors, or harmful to the Company or its customers, if disclosed. It also includes information that suppliers and customers have entrusted to us.

Protection and Proper Use of Company Assets

All Company Personnel should endeavour to protect the Company's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability. Any suspected incidents of fraud or theft should be immediately reported for investigation.

Company assets, such as funds, products or computers, may only be used for legitimate business purposes or other purposes approved by management. Company assets may never be used for illegal purposes.

The obligation to protect Company assets includes proprietary information.

Proprietary information includes any information that is not generally known to the public or would be helpful to our competitors. Examples of proprietary information include intellectual property, such as trade secrets, patents, trademarks and copyrights, as well as business, marketing and service plans, engineering and manufacturing ideas, designs, databases, records, salary information and any unpublished financial data or reports. Unauthorized use or distribution of this information is a violation of Company policy. It may also be illegal and may result in civil and criminal penalties. The obligation to preserve proprietary information continues even after you leave the Company.

Fair Dealing

We seek to outperform our competition fairly and honestly. We seek competitive advantages through superior performance, never through unethical or illegal business practices. Stealing proprietary information, possessing trade secret information obtained without the owner's consent or inducing the disclosures of proprietary information or trade secrets by past or present employees of other companies is prohibited. Company Personnel should endeavour to deal fairly with the Company's customers, suppliers, competitors and employees. Company Personnel should not take unfair advantage of anyone through illegal conduct, manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair-dealing practice.

Discrimination and Harassment

We value the diversity of our Company Personnel and are committed to providing equal opportunity in all aspects of employment. Abusive, harassing or offensive conduct is unacceptable, whether verbal, physical or visual. Examples include derogatory comments based on racial or ethnic characteristics and unwelcome sexual advances. Company Personnel are encouraged to speak out when a co-worker's conduct makes them uncomfortable, and to report harassment when it occurs.

Safety and Health

We are all responsible for maintaining a safe and healthy workplace by following safety and health rules and practices. The Company is committed to keeping its workplaces free from hazards. Please report any accidents, injuries, unsafe equipment, practices or conditions immediately to a supervisor or other designated person. Threats or acts of violence or physical intimidation are prohibited.

In order to protect the safety of all employees, Company Personnel must report to work in condition to perform their duties and free from the influence of any substance that could prevent them from conducting work activities safely and effectively. The use of illegal drugs in the workplace is prohibited.

Financial Statements and Recordkeeping

Honest and accurate recording and reporting of information is critical to our financial reporting and our ability to make responsible business decisions. The Company's accounting records are relied upon to produce reports for the Company's management, shareholders, creditors, governmental agencies and others. Our financial statements and the books and records on which they are based must truthfully and accurately reflect all corporate transactions and conform to all legal and accounting requirements and our system of internal controls.

A separate Code of Ethical Conduct for Financial Managers forms part of this Code as Schedule "A".

All Company Personnel have a responsibility to ensure that the Company's records, including accounting records, do not contain any false or intentionally misleading entries. We do not permit intentional misclassification of transactions as to accounts, departments or accounting periods. All transactions must be supported by accurate documentation in reasonable detail and recorded in the proper account and in the proper accounting period.

All Company books, records, accounts and financial statements must be maintained in reasonable detail, must appropriately reflect Company transactions and must conform to both applicable legal requirements and the system of internal controls of the Company. Unrecorded or "off the books" funds or assets should not be maintained unless permitted by applicable laws or regulations.

Business records and communications may become public through legal or regulatory investigations or the media. We should avoid exaggeration, derogatory remarks, legal

conclusions or inappropriate characterizations of people and companies. This applies to communications of all kinds, including email and informal notes or interoffice memos. Records should be retained and destroyed in accordance with the Company's records storage and retention policy.

Use of E-Mail and Internet Services

E-Mail systems and Internet services are provided to help us do work. Incidental and occasional personal use is permitted, but never for personal gain or any improper purpose. You may not access, send or download any information that could be insulting or offensive to another person, such as sexually explicit material or jokes, unwelcome propositions, ethnic or racial slurs, or any other message that could be viewed as harassment. Also remember that "flooding" our systems with junk mail and trivia hampers the ability of our systems to handle legitimate Company business and is prohibited.

Company Personnel should not download copyrighted materials, should not copy material that is not licensed to the Company and should follow the terms of a license when using material that is licensed to the Company. No changes should be made to licensed materials without the prior consent of the Company. In addition, Company Personnel are discouraged from downloading games and screensavers, as these are common sources of viruses.

Your messages (including voice mail) and computer information are considered the Company's property and you should not have any expectation of privacy. Unless prohibited by law, the Company reserves the right to access and disclose this information as necessary for business purposes. Use good judgment, and do not access, send messages or store any information that you would not want to be seen or heard by other individuals.

Please refer to the Information Technology Acceptable Use Policy attached hereto as Schedule "B" for additional information.

Political Activities and Contributions

We respect and support the right of our Company Personnel to participate in political activities. However, these activities should not be conducted on Company time or involve the use of any Company resources such as telephones, computers or supplies. Company Personnel will not be reimbursed for personal political contributions.

We may occasionally express our views on local and national issues that affect our operations. In such cases, Company funds and resources may be used, but only when permitted by law and by our strict guidelines. The Company may also make limited contributions to political parties or candidates in jurisdictions where it is legal and customary to do so. Company Personnel may not make or commit to political contributions on behalf of the Company without the approval of the Board of Directors.

Gifts and Entertainment

Business gifts and entertainment are customary courtesies designed to build goodwill among business partners. These courtesies include such things as meals and beverages, tickets to

sporting or cultural events, discounts not available to the general public, travel, accommodation and other merchandise or services. In some cultures they play an important role in business relationships. However, a problem may arise when such courtesies compromise – or appear to compromise – our ability to make objective and fair business decisions.

Offering or receiving any gift, gratuity or entertainment that might be perceived to unfairly influence a business relationship should be avoided. These guidelines apply at all times, and do not change during traditional gift-giving seasons. No gift or entertainment should ever be offered, given, provided or accepted by any director or employee of the Company, or by any family member of a director or employee, unless it (1) is not a cash gift, (2) is consistent with customary business practices, (3) is not excessive in value, (4) cannot be construed as a bribe or payoff and (5) does not violate any applicable laws or regulations. Please discuss with your supervisor any gifts or proposed gifts if you are uncertain whether they are appropriate.

Waivers of This Code of Business Conduct and Ethics

Any waiver of this Code with respect to a director or executive officer of the Company may be made only by the Board of Directors or the Audit Committee. Any such waiver will be promptly disclosed to the extent required by applicable laws or stock exchange regulations.

Reporting of any Illegal or Unethical Behaviour

We have a strong commitment to conduct our business in a lawful and ethical manner. Company Personnel are encouraged to talk to supervisors, managers or other appropriate personnel when in doubt about the best course of action in a particular situation. You have the right and the responsibility to report suspected violations of this Code. Company Personnel making such reports in good faith will have the full support of the Company. If you have knowledge or are suspicious of any non-compliance with this Code or are concerned whether circumstances could lead to a violation of this Code, discuss the situation with your immediate supervisor. If the circumstances are such that it would be inappropriate to involve your immediate supervisor, you should contact the Chairman of the Audit Committee.

Compliance Procedures

This Code cannot, and is not intended to, address all of the situations you may encounter. There will be occasions where you are confronted by circumstances not covered by policy or procedure and where you must make a judgment as to the appropriate course of action.

Since we cannot anticipate every situation that may arise, it is important for the Company to set forth a general way to approach a new question or problem. The following steps should be kept in mind when determining the appropriate course of action:

1. *Make sure you have all of the facts.*

In order to reach the right solutions, you must be as fully informed as possible.

2. *Ask yourself what you are specifically being asked to do.*

This analysis will enable you to focus on the specific issues that are raised and the available alternatives. Use your judgment and common sense. If something seems unethical or improper, it probably is.

3. *Clarify your responsibility and role.*

In most situations, there is shared responsibility. Are your colleagues informed? It may help to get others involved and to discuss the problem.

4. *Discuss the problem with your supervisor.*

This approach is best in most if not all situations. Your supervisor may be more knowledgeable about the issue and will appreciate being brought into the process. It is a supervisor's responsibility to help you to solve problems.

5. *Seek help from Company resources.*

In the rare instance in which it may not be appropriate to discuss an issue with your supervisor, or in which you feel uncomfortable approaching your supervisor, discuss the problem with the Company's Corporate Secretary. If you prefer to write, address your concerns to the Company's Corporate Secretary or the Chief Executive Officer.

6. *You may report ethical violations in confidence and without fear of retaliation.*

If your situation requires that your identity be kept secret, the Company will protect your anonymity. The Company does not permit retaliation of any kind against Company Personnel for good faith reports of ethical violations. An officer or employee who retaliates against someone who has reported an ethical violation in good faith is subject to discipline up to and including termination of employment. These procedures are intended to encourage and enable Company Personnel and others to raise serious concerns within the Company rather than seeking resolution outside the Company.

7. *Ask first.*

If you are unsure of the proper course of action, seek guidance before you act. If you do not feel comfortable discussing the matter with your supervisor, please call the Company's Corporate Secretary or call the Compliance Hotline for anonymous reporting that will be directed to the Chairman of the Audit Committee or other appropriate persons. The Compliance Hotline is answered by an outside service provider and is available to all Company Personnel. If you require an interpreter, every reasonable effort will be made to provide you with one. We strive to ensure that all questions or concerns are handled fairly, discreetly and thoroughly.

Approved by the Board of Directors on the 19th day of February, 2009.

Schedule "A"

CODE OF ETHICAL CONDUCT FOR FINANCIAL MANAGERS

Introduction

This Code of Ethical Conduct for Financial Managers ("Code") applies to all Financial Managers of Crosshair Exploration & Mining Corp. (the "Company"). Financial Managers are the Company's principal executive officer, principal financial officer, principal accounting officer, controller or person performing similar functions.

This Code covers a wide range of financial and non-financial business practices and procedures. This Code does not cover every issue that may arise, but it sets out basic principles to guide all Financial Managers of the Company. If a law or regulation conflicts with a policy in this Code, the Financial Manager must comply with the law or regulation. If a Financial Manager has any questions about this Code or potential conflicts with a law or regulation, they should contact the Company's Board of Directors, Audit Committee or Corporate Secretary.

Each Financial Manager shall recognize that Financial Managers hold an important and elevated role in corporate governance. They are uniquely capable and empowered to ensure that the Company's, its stockholders' and other stakeholders' interests are appropriately balanced, protected and preserved. Accordingly, this Code provides principles to which Financial Managers are expected to adhere and advocate. The Code embodies rules regarding individual and peer responsibilities, as well as responsibilities to the Company, the stockholders, other stakeholders and the public.

Financial Code Principles and Responsibilities

Financial Managers shall adhere to and advocate to the best of their knowledge and ability the following principles and responsibilities governing their professional and ethical conduct.

1. Act with honesty and integrity, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships. A "conflict of interest" exists when an individual's private interests interfere or conflict in any way (or even appear to interfere or conflict) with the interests of the Company.
2. When disclosing information to constituents, provide them with information that is accurate, complete, objective, relevant, timely and understandable. Reports and documents that the Company files with the B.C. Securities Commission, the U.S. Securities and Exchange Commission or other regulatory authority, or releases to the public shall contain full, fair, accurate, timely and understandable information. The principal executive officer and principal financial officer shall review the annual and quarterly reports, certify and file them with the appropriate regulatory authorities.
3. Comply with the laws, rules and regulations of Canadian and U.S. federal, state, provincial and local governments, and other appropriate private and public regulatory agencies including any stock exchanges upon which the Company's securities are traded.

4. Act in good faith, responsibly, with due care, competence and diligence, without misrepresenting material facts or allowing their independent judgment to be subordinated.
5. Protect and respect the confidentiality of information acquired in the course of their work except when authorized or otherwise legally obligated to disclose. Confidential information acquired in the course of their work shall not be used for personal advantage.
6. Achieve responsible use of and control over all assets and resources employed by or entrusted to them.
7. Promptly report Code violations to the Company's Chairman of the Board and Audit Committee Chairman.

Waivers of the Code

Any waiver of this Code for Financial Managers may be made only by the Audit Committee of the Board of Directors and will be promptly disclosed as required by law or the private regulatory body. Requests for waivers must be made in writing to the Company's Chairman of the Board and Audit Committee Chairman prior to the occurrence of the violation of the Code.

Reporting of Violations of the Code, Illegal or Unethical Behaviour

Financial Managers should report observed violations of the Code and illegal or unethical behaviour to the Company's Chairman of the Board and Audit Committee Chairman. All reports will be treated in a confidential manner and it is the Company's policy to not allow retaliation for reports made in good faith of misconduct by others. The Company's Audit Committee will lead all investigations of alleged violations or misconduct. Financial Managers are expected to cooperate in internal investigations of misconduct and violations of this Code.

Violations of the Code

Financial Managers who violate the standards of this Code will be subject to disciplinary action, which may include termination of employment, civil action and/or referral to law enforcement agencies for criminal prosecution.

Schedule “B”

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

1. Overview

The intention of this document is to provide a framework that offers an environment that users can work together. The framework is designed to prevent security breaches and protect the company and users from illegal or damaging actions whether intentional or unintentional.

There are countless threats that could damage the network. It is impossible to list all the actions that could pose a threat. Users of the network are required to exercise good judgment and act in good faith.

All the rules are based on best security practices and are implemented for a very good reason.

2. Considerations

When defining an “Acceptable Use and Security Policy” several factors need to be taken into account. The key questions that need to be asked in defining a framework:

- a. What happens if the network security is breached?
- b. What are the financial implications?
- c. What are the public relation implications?
- d. What are the trust implications in the market place?
- e. Who is accountable should the network be breached?
- f. How does one determine who is responsible?
- g. How can a security policy be enforced?
- h. What type of work environment users can operate in?

Crosshair Exploration is a publically listed company trading on Stock Exchanges in both Canada and the United States. A listed company has many statutory requirements to keep information confidential until it is officially made available to the broad public. An information leak could have serious consequences in the market place including financial losses, unnecessary market turmoil and ill founded rumours.

Crosshair Exploration is also a company that would like to create a work environment that is pleasant to work in, and which allows some flexibility to use the corporate technology infrastructure for necessary personal use.

To ensure that Crosshair Exploration meets its statutory requirements of keeping information confidential until it is officially made public, Crosshair Exploration has decided to enforce a high level of security.

3. Scope

This document scope covers any device or piece of equipment that connects directly or indirectly to the Crosshair Exploration network. The devices include, but are not limited to:

- Crosshair Exploration workstations
- Crosshair Exploration servers
- Crosshair Exploration network devices
- User's personal computers that directly or indirectly connect to the corporate network
- Networking services provided both internally by Crosshair Exploration and externally by third party suppliers

This policy also applies to all users that connect directly or indirectly to the Crosshair Exploration network. The users include, but are not limited to:

- Management
- Employees
- Partners and investors
- Suppliers
- Devices that use the network

4. Terminology

For the purpose of this policy, the following convention will be used:

- "Network" refers to the Crosshair Exploration network and any device that is directly or indirectly connected to it.
- "Systems administrator" refers to the organization/person(s) who has been appointed by management to administer and manage the network.
- "Users" refers to any user or device that is directly or indirectly connected to the network.
- "Information" refers to, but is not limited to, any data, piece of thereof, documents, programmes, software

5. Enforcement

Those in violation of the standards set forth in this policy will be subject to disciplinary action up to and including dismissal

6. Policies

6.1 General policies

- 6.1.1 Responsibility: Users are responsible for all actions that they perform on the network or devices connected directly or indirectly to the network. Where a policy is not in place, users are required to request written permission from the systems administrator before performing any actions outside the scope of this document. In addition users are required to exercise sound judgement and good faith when using and accessing the Crosshair Exploration network.
- 6.1.2 Use of the network: The network may only be used to the benefit of Crosshair Exploration. Any activities that do not benefit the Crosshair Exploration are prohibited.
- 6.1.3 Netiquette: Users are required to exercise good netiquette, and use the network and Internet in way that is responsible, considerate and fair to all concerned in order to preserve a positive company image. Examples include, but not limited to: blogs, forums, newsgroups and email.
- 6.1.4 Personal use: Crosshair understands that there may be times when the network, internet and email resources may be needed and utilized for personal reasons. Crosshair expects that personal use is kept to a minimum and that employees utilize good and appropriate judgment at all times. All activities must conform to the acceptable use specified in this is document. The user assumes all risks in the use of Crosshair Exploration's network for personal use.
- 6.1.5 Illegal use: The network may not be used for any illegal or fraudulent activities whether directly on indirectly.
- 6.1.6 Labour laws: The network may not be used for any activities which are in contravention to the labour laws including, but not limited to, sexual harassment laws and jurisdictional industry labour laws, etc.
- 6.1.7 Harassment: The network may not be used for harassment of any kind whether using unprofessional language and high frequency communication.
- 6.1.8 Disrupting services: No process or activity may be performed that is intended to disrupt network services.
- 6.1.9 Permissions: No activity that changes the permissions on the network may be performed without the written consent of the security administrator.

6.2 Information and proprietary information policy

- 6.2.1 Ownership: All information on the network is the property of Crosshair Exploration.
- 6.2.2 Storage: Only information that is owned by Crosshair Exploration may be stored on the network.
- 6.2.3 Storage location: All information must be stored on the Crosshair Exploration servers. No information is to be stored locally on the workstations.
- 6.2.4 Deletion of information: No information that belongs to Crosshair Exploration may be deleted.
- 6.2.5 Copying and dissemination: No unauthorized information may be copied or distributed by any means including, but not limited to: digital copying, digitizing,

photocopying, photography, showing/telling someone the information on the screen.

- 6.2.6 Software: Only software that is owned by Crosshair Exploration and has the appropriate active licenses may be installed and used. No personal software or licenses may be used on the network.
- 6.2.7 Exporting software: Exporting software, encryption algorithms, technology, and designs to countries that are restricted by export laws is illegal and prohibited.
- 6.2.8 Warranty statements: No warranty statements may be made without the written permission of management. Examples include, but not limited to stock price speculations and public information releases.
- 6.2.9 Providing information on the network: No information may be communicated or hinted upon in any way regarding:
 - Suppliers for hardware and software
 - Configuration
 - Installation and set up
 - Time frames, including release of new and updated network services
 - Service providers
 - Support and system administration staff
 - Contracts
 - Passwords
- 6.2.10 Communication of confidential information: No confidential information may be communicated to any party or organization without the use of secure communication process that has been approved by the system administrator. Confidential information includes, but not limited to passwords, financial statements, pre-public information, pre-news releases, designs and engineering drawings.
- 6.2.11 Information transportation: Information may only be transported on removable media with the written authorization of management and using encryption tools authorized by the systems administrator.
- 6.2.12 Postings: When, as part of the job function, users post information onto newsgroups, forums, email lists and alike, they must include a disclaimer stating that it is strictly their own opinion and not of Crosshair Exploration.

6.3 Device policies

Scope: Any device that connects to the network. Examples include, but are not limited to: workstations, servers and network devices

- 6.3.1 Administrative control: Users may not remove or change the ability for system administrators to fully control and administer the device.
- 6.3.2 Disabling of services: No device service or application may be disabled that is designed to protect the network and administer the network without the written permission of the system administrator. Examples include, but are not limited to: Antivirus, firewall, and administrative control applications.
- 6.3.3 Communication: While using the network, no communication with any device, whether direct or indirect, may be performed without the written permission of

the systems administrator. Examples include, but are not limited to: messaging programmes (e.g. MSN Messenger, Yahoo Messenger, Skype), web servers, FTP servers, iPods, USB drives, etc.

- 6.3.4 Software installation: No software may be installed without the written permission from the systems administrator.
- 6.3.5 Running applications: No unauthorized application may be run on the network without the written approval from the system administrator. This includes, but not limited to: scripts, programmes, ActiveX controls, packages and executables of any kind.
- 6.3.6 Screen savers: A password protected screen saver must be activated within 5 minutes of leaving the device unattended.
- 6.3.7 Core services: All workstations must have the corporate antivirus scanner and corporate security software installed. In addition a root scan must be run before the machine can become active on the network.
- 6.3.8 Internet browsing: Only websites that are business related and are related to the business of Crosshair Exploration. Visiting websites such as, but not limited to: illegal content, pornographic content and racial slanted content; is strictly prohibited.

6.4 Email communication policies

- 6.4.1 Email Use: Corporate email may only be used for business purpose and for the benefit of Crosshair Exploration.
- 6.4.2 Language: Only professional business language may be used in correspondence.
- 6.4.3 Advertising: No advertising of any sorts may be performed. This includes, but is not limited to: stock touting (even to the so called “benefit” of Crosshair Exploration), selling or promoting goods and services, promoting persons, unsolicited email, communicating with someone that is legally not allowed to receive correspondence etc.
- 6.4.4 Chain letters: The creation and or forwarding of chain letters. Examples include: chain letters, pyramid, ponsy schemes and jokes.
- 6.4.5 Spam: The creation and/or response to Spam email are strictly prohibited.
- 6.4.6 Stationery, fonts and signatures: Only the standard email stationery, fonts and signatures may be used.
- 6.4.7 Email address: Only the email address supplied by the system administrator to the user may be used to conduct Crosshair Exploration email communication.
- 6.4.8 Spoofing email addresses: No emails may be sent out through impersonation of another email address. This includes, but not limited to, changing email headers and tampering with the email message.
- 6.4.9 Confidential information: No confidential information may be emailed. Confidential information includes, but is not limited to passwords, financial statements, pre-public information, pre-news releases, designs and engineering drawings, drilling locations, customer information. (Email is not secure)
- 6.4.10 Email client: Only the approved email client may be used. Currently this is Outlook 2007 and webmail.
- 6.4.11 Opening attachments: No executable attachment may be opened. Examples include not limited to: files with executable extensions (exe, com, bat, cmd, vbs,

pl), mdb, xla, macro files embedded in Word, Excel and PowerPoint. All attachments must be saved first to disk to allow for examination by the user and antivirus.

6.4.12 Opening email from unknown senders: Extreme caution must be applied to opening email messages from unknown senders. If in doubt, please contact the systems administrator who will use the necessary precautions.

6.5 Privacy and monitoring

6.5.1 Access to information: The system administrator has access to all information. Particular discretion will be applied to aspects that are deemed private. Examples included, but are not limited to: salary, compensation packages, financial statements, pre-release public press releases, email, strategies, designs and anything that appears to be confidential.

All information on the corporate network is public only to employees. Management at their discretion have the right to monitor and/or make any of the information available to any user of choice.

6.5.2 Monitoring of networking activities: The system administrator monitors the network to get an advance warning of impending threats and to enhance the network for the benefit of all users. The following is a non limitative list of services and information that may be monitored at any time:

- Website browsing including Internet and Intranet
- File Transfer Protocol activities (FTP)
- Communication with internal and external devices
- Services that are critical to the security of the network e.g. antivirus and security software
- Monitoring of activities on a computer, including everything that a user sees on the screen
- Email
- File access, creation and, modification
- Network services
- Remote access connections
- Messaging applications
- Unauthorized use of the network, especially applications that either use unusual ports or unusual communication protocols on ports that are designed for other protocols or applications that are known offenders on the network.
- File scanning
- Applications installed on a device
- Processes running on the device
- The use of encryption or lack thereof
- Sniffing for specific network traffic “keywords”
- Changing permissions
- Analysis of network traffic

6.6 Network policies

- 6.6.1 Malicious software: It is prohibited to introduce any malicious software onto the network. Examples include, but are not limited to, Trojans, viruses, malware, email bombs
- 6.6.2 Hacking: Hacking into a network both internal and external to Crosshair Exploration's network is illegal and prohibited. Users may only access information that they have been assigned permission to access. Examples include, but are not limited to
- Circumventing authentication systems
 - Trying different user names and passwords to gain unauthorized access to systems or information whether manually, using software, scripts and alike.
- 6.6.3 Prohibited networking activities: The following network activities are strictly prohibited on the network:
- Network sniffing and monitoring
 - Port scanning
 - Flooding the network including, but not limited to, socket dumps, ping floods, multiple socket connects and disconnects and multiple hanging connects and protocol dumps not specified for a device
 - Any form of denial of service (DOS) attacks
 - Packet spoofing
 - Spoofed routing
 - IP spoofing
 - Routing
 - Dual homing
 - Security scanning
 - Network service scanning
 - Any form of information spoofing
 - Any network activity that has a malicious intent
 - Intercepting any data that is not specifically intended for the user
- 6.6.4 File sharing: No peer-to-peer file sharing is allowed. This includes creating local shares on workstations to share files with other users. Using peer-to-peer software such as, but not limited to, Limewire and Kazaa, is prohibited.
- 6.6.5 Connecting equipment: No equipment may be connected to the network without the written permission of the system administrator. This includes, but is not limited to: computers, Blackberries and network enabled devices.

6.7 Password policies

- 6.7.1 Secrecy: Passwords must be kept secret at all times. Only the user who has authorized access may have the credentials to log in to authorized systems and devices. Passwords may not be shared with anyone and includes any method whereby a password can be derived.
- 6.7.2 Storage of password: Passwords may not be noted anywhere. This includes, but not limited to notepads, books, documents, files, filenames, online and websites.

Passwords must be remembered or stored in a software password safe authorized by the system administrator.

6.7.3 Responsibility: All actions from a specified user that damage or impact the network negatively are the responsibility of the specified user.

6.7.4 Password complexity: Password used on the network must conform to the following:

- At least 8 characters long
- Contains at least one upper case (A to Z)
- Contains at least one lower case (a to z)
- Contain at least one number (0 to 9)

6.7.5 Password content: The contents of a password must conform to the following:

- May not be a password example used in this document
- May not contain the personal information such as names of users, family, pets, cities, countries, friends, telephone numbers and birthdates
- May not contain the words God, password and username
- May not be words in any language to prevent dictionary attacks

Strong password example: uTwe2f24Hr

Weak password example: DonalDuck1234

6.7.6 Password changes: Passwords must be changed every 45 days to a new password that has not been used in the last year.

6.7.7 Reusing passwords: The same passwords may not be used to access different sites.

6.8 Remote access policy

6.8.1 Secure tunnel: All access from users outside of the corporate must go through a secure tunnel. The only authorized secure tunnel is the to Crosshair Exploration VPN tunnel

6.8.2 Information access: Crosshair Exploration may only be accessed via remote desktop. No information may be copied to the local machine. This does not include personnel required to travel.

6.8.3 Drive mapping: No drive of any sort may be mapped to the remote desktop connection.

6.8.4 Clearing temporary files: After the remote session is complete, all temporary files and unused space must be cleared using secure delete program authorized by the system administrator.

6.8.5 Security: Devices connecting remotely must have an active and current antivirus and firewall that is approved by the systems administrator. The network that the remote device is connecting from must adhere to the same policies described in this document.

6.8.6 Dual homing: The device that is remotely connecting to the Crosshair Exploration may not be connected to another network for dual homing and/or routing purposes.

6.9 Laptop users

6.9.1 Backup: Staff that has corporate data on their laptop, and in the absence of an automated backup process; are responsible for backing up their data to the server on a weekly basis. The data includes, but not limited to: corporate data and email.

Crosshair Exploration & Mining Corp.

And its Subsidiaries and Affiliates

Code of Ethics and Business Conduct

Compliance Certificate

I have read and understand the Code of Ethics and Business Conduct of Crosshair Exploration & Mining Corp. (“Crosshair”). I will adhere in all respects to the standards described in the Code. I further confirm my understanding that any violation of the Code will subject me to appropriate disciplinary action which may include but not be limited to, my demotion, discharge or termination or termination of my consulting contract with Crosshair.

I confirm to Crosshair that I am not in violation on the Code, except as pertains to the exceptions attached hereto.

Date: _____

Signature: _____

Name: _____