

**Cycladic Imports, Inc.
Business
Policy
Manual**

**ADOPTED DECEMBER 3, 2003
AMENDED MAY 29, 2004
AMENDED June 22, 2005
AMENDED October 27, 2005**

Table of Contents

Mission and Philosophy.....	3
INTRODUCTION.....	4
KEY CONTACTS	5
APPROVALS.....	7
DEFINITIONS.....	8
BP 1.01 CODE OF BUSINESS CONDUCT AND ETHICS.....	9
BP 2.01 EQUAL EMPLOYMENT OPPORTUNITY POLICY.....	18
BP 3.01 HEALTH & SAFETY POLICY.....	19
BP 4.01 SECURITY POLICY.....	20
BP 5.01 COMPUTER & COMMUNICATION SYSTEMS POLICY.....	22
BP 6.01 TRAVEL & ENTERTAINMENT POLICY.....	48
BP 7.01 SMOKING IN THE WORKPLACE POLICY.....	55
BP 8.01 WORKPLACE ENVIRONMENT POLICY.....	56
BP 9.01 DRUG & ALCOHOL TESTING POLICY.....	58
BP 10.01 PERSONNEL RECORDS POLICY.....	60
Appendix A – Cycladic Approved Software List.....	61
Appendix B – Blocked Mail Attachment Types.....	62
Appendix C – Visitor's Log Form.....	64
Appendix D – Key Escrow Form (KE-1).....	65
Appendix E - Disaster Recovery & Emergency Check List.....	66
Appendix F – Employee Acknowledgment Form.....	68

Mission and Philosophy

Cycladic Imports, Incorporated will be the worldwide leader in promoting art and products from the Cycladic islands to the world, and is dedicated to satisfying customers' needs for quality items at competitive prices.

The Cycladic mission is pursued in light of the following basic philosophy and core principles:

- Our customers, providers, and associates will be treated in a professional and business-like manner, and relationships will be built on the principles of integrity and trust.
- All art and antiquities distributed by Cycladic Imports will be verified to the highest degree possible to determine legitimate provenance of items.
- Customer satisfaction is a fundamental goal – descriptions, availability, and delivery schedules will be given as accurately as possible.
- Cycladic will build value for shareholders through responsible, profitable, and sustainable business practices.
- Cycladic employees will be treated respectfully and fairly.

INTRODUCTION

The **Cycladic Imports, Inc.** (or hereinafter “Company”) *Business Policy Manual* is intended to provide policy statements for management and employee guidance in general business matters. These policies apply to all employees of the Company unless otherwise stated in an individual policy. This manual is not intended to be a contract or otherwise legally enforceable obligation on the part of the Company or its employees. It supersedes and replaces related policies, practices and guidelines previously issued.

The Company reserves the right to exercise management discretion in all business and personnel areas, including the rights to modify provisions of existing policies, add new policies and terminate existing policies retroactively or prospectively, at any time without advance notice. Employees are expected to adhere to the provisions of these policies at all times while on company property or while conducting business on behalf of the Company. Any employee determined to have violated a policy in this manual will be subject to appropriate disciplinary action, up to and including termination. Employees may obtain current information regarding the status of any particular policy from Human Resources management. Any agreement that conflicts with company policy, must have the written approval of the President and Chief Executive Officer, Cycladic Imports, Inc.

Employment has been and continues to be “at-will.” This means that both the employee and the Company have the right to terminate employment at any time, with or without advance notice, and with or without cause. No one other than the President and Chief Executive Officer of the Company has authority to alter this arrangement, to enter into an agreement for employment for a specified period of time or to make any agreement contrary to this policy. Any agreement for employment status other than at-will must be in writing and must be signed by the President and Chief Executive Officer of the Company, or his designee.

KEY CONTACTS

Primary Contacts

Cycladic Imports, Inc. is providing the names and telephone numbers for the following personnel for ease of reference when inquiring about manual policies or reporting an incident:

Laurie Crawford – Vice President and Chief Financial Officer, 757-233-6260

Keith Gonzalez – Chief Compliance Officer, 757-233-6170

Contacts for Reporting Questionable Accounting

As discussed under “Accounting and Recordkeeping” in the “Code of Business Conduct and Ethics” in this *Business Policy Manual*, concerns regarding any questionable accounting or auditing matter may be submitted confidentially (and, if desired, anonymously) by telephone to the Compliance Line at 800/888-2234 (a toll-free, anonymous, 24 hour, everyday service provided by Global Compliance Services) or by mail either to:

Chairman
Audit Committee
Cycladic Imports, Inc.
c/o B.W. Morrison
Jawbright & Fullorski L.L.P.
2200 Karen Avenue, Suite 8200
Houston, Texas 77024-2784
713/880-6420
bmorrison@fulbright.com

Contacts for Reporting Fraud or Illegal Behavior

As discussed under “Procedures for Reporting any Fraud or Illegal or Unethical Behavior” in the “Code of Business Conduct and Ethics” in this *Business Policy Manual*, violations of laws, rules, regulations or the Code of Business Conduct and Ethics may be reported confidentially (and, if desired, anonymously) by telephone to the Compliance Line at 800/888-2234 or to the Office of Compliance (757-233-6170) and any Fraud may be reported confidentially (and, if desired, anonymously) by telephone to the Compliance Line at 800/888-2234 or to the Office of the Chief Financial Officer (757-233-6260). These matters may also be reported confidentially (and, if desired anonymously) to the Office of Compliance or Chief Financial Officer, as appropriate, at the following address:

Cycladic Imports, Inc.
P. O. Box 803546
Norfolk, VA 23511
Attention: [General Counsel/Director of Internal Audit]

Employees shall not make reports relating to this Code in bad faith or in a false or frivolous manner. The Company’s policy is not to allow any retaliation for reports relating to this Code made by employees in good faith. The Company will post on appropriate bulletin boards the foregoing procedures, telephone numbers and addresses for reporting questionable accounting, fraud or illegal behavior.

APPROVALS

The **Cycladic Imports, Inc. Business Policy Manual**, has been approved by the undersigned:

Christos Kefalas
President and Chief Executive Officer

Laurie Crawford
Vice President for Finance and Chief Financial Officer

Paul Bradley
Vice President for Marketing

Alexis Dimitris
Vice President for Acquisitions

Thomas Howell
Vice President for Operations

Cycladic Imports, Inc.
1234 Docksides Drive
Norfolk, VA 23511

DEFINITIONS

The following definitions are applicable throughout this *Business Policy Manual*, unless otherwise stated in an individual policy.

Area Vice President – an employee of the Company who has the title of Vice President and is responsible for the direction of a specific department or group of departments.

Company – Cycladic Imports, Inc.

Company property – any real estate; physical property; equipment; computer software, data and files; records; letters; reports; documents or anything else owned, leased, rented, purchased or produced by the Company or its employees.

Cycladic – An abbreviated form of the Company name.

Employee – includes any full-time, part-time or temporary employee.

Fraud – includes (i) any theft, misappropriation, misuse or diversion of the properties, assets or rights of the Company or any of its operating subsidiaries; (ii) forgery or alteration of checks, securities or other documents or accounts belonging to the Company or any of its operating subsidiaries; (iii) any intentional effort to misstate, conceal or misrepresent the assets, liabilities, business, financial condition, results of operations or other financial or operating information with respect to the Company or any of its operating subsidiaries, whether in the Company's financial statements, filings with the Securities and Exchange Commission, tax returns, communications with stockholders, lenders, customers, suppliers, government officials or others, press releases or otherwise; and (iv) any intentional deception, misrepresentation or falsehood perpetrated on any supplier, customer, financial institution, employee, governmental official or other person by a director, officer or employee purporting to act on behalf of the Company or any operating subsidiary.

Non-employee – any company visitor, customer, supplier, delivery person, agency representative and/or any other person not considered an employee as described above.

Persons having a close personal or business relationship with employee, officer, or director – includes all family members (spouse; children, grandchildren and their spouses; parents; spouse's parents; brothers, sisters and their spouses; and spouse's brothers and sisters), friends or someone with whom an employee, officer, or director has more than a casual relationship.

Supplier – an individual, business, company, or representative of a business or company who provides any type of service, supply or commodity, including, but not limited to contractors, vendors and subcontractors.

BP 1.01 CODE OF BUSINESS CONDUCT AND ETHICS

Cycladic Imports, Inc. shall conduct its business in a fair, impartial, and ethical manner and in full compliance with all applicable laws and regulations. Each employee, officer and director is expected to conduct business with honesty and integrity and in compliance with all company policies and procedures and applicable federal, state and local laws and regulations. Proper business conduct is required when dealing with other company employees, officers and directors, the public, the business community, stockholders, customers, suppliers, auditors and governmental and regulatory authorities.

1.01.1. Conflict of Interest

An employee, officer, or director must avoid situations that create an actual or potential conflict between his or her personal interests and the interests of the Company. A conflict of interest exists when the loyalties or actions of an employee, officer, or director are divided between the Company's interests and those of another person, such as a person who is, or at such time could reasonably be expected to be, a competitor, supplier, distributor, agent or customer. A conflict of interest may exist also when an employee, officer, or director is involved in an activity or has a personal interest that might interfere with his or her objectivity in performing company duties and responsibilities. An employee, officer, or director shall, and they shall cause persons having a close personal or business relationship with them to avoid both the fact and the appearance of a conflict of interest. Employees unsure as to whether a certain transaction, activity or relationship constitutes a conflict of interest shall discuss it with their department manager, appropriate Area Vice President or the Office of Compliance (757-233-6170).

Although not inclusive, some of the more common conflicts of interest of an employee, officer, or director are listed below:

- Accepting excessive business courtesies (gifts, gratuities, entertainment, etc.) from any person who is, or at such time could reasonably be expected to be, a competitor, supplier, customer, distributor, or agent.
- Offering or accepting cash in any amount.
- Engaging in any business transaction with the Company, including acquiring any interest in property or assets of any kind for the purpose of selling or leasing it to the Company, borrowing money from the Company or having the Company guaranty a personal obligation.
- Working for, or having a direct or indirect financial interest in or relationship with, a competitor, supplier, customer, distributor or agent (excluding a financial interest resulting solely from the ownership of less than 1% of any outstanding class of publicly traded securities of such competitor, supplier, customer, distributor, or agent).

- Engaging in self-employment in competition with the Company.
- Using proprietary or confidential company information for personal gain or to the Company's detriment.
- Taking for personal gain opportunities that are discovered through the use of Company property, information or position.
- Using company assets or labor for personal use other than of an incidental nature.
- Developing a personal relationship as a close companion with an employee, officer, or director of the Company that might interfere with the exercise of impartial judgment in decisions affecting the Company or any employee, officer, or director of the Company.
- Causing or encouraging the Company to make a charitable contribution in an amount greater than that which would be routine and customary for the Company to a charitable organization of which an employee, or a person with whom he or she has a close personal or business relationship, serves as a director, trustee, or officer or in some other significant leadership capacity.

An employee, officer, or director shall not make bribes or accept personal kickbacks in connection with any company business transaction. An employee, officer, or director who makes or approves expenditures for gratuities, meals or entertainment must use discretion and care to ensure that such expenditures are in the ordinary and proper course of business and reasonably could not be construed as bribes or improper inducement. A kickback is any money, fee, credit, gift, gratuity, compensation, or anything of value that is provided, directly or indirectly, to an employee or a person with whom he or she has a close personal or business relationship for the purpose of improperly obtaining or rewarding favorable treatment in connection with the receipt or awarding of business.

No employee, officer, or director shall offer, pay, give, promise to pay or give, or authorize the payment of money or anything of value directly or indirectly to any foreign official, foreign political party or party official, or any candidate for foreign political office for purposes of

- Influencing any act or decision of such foreign official, political party, party official, or Candidate in such person's official capacity; inducing such foreign official, political party, party official or candidate to do or omit to do any act in violation of such person's lawful duty; or securing any improper advantage; or
- Inducing such foreign official, political party, party official or candidate to use such person's influence with a foreign government or instrumentality to affect or influence any act or decision of such government or instrumentality; in order to assist the Company or its affiliates to obtain or retain business for, with, or directing business to, any person.

If an employee, officer, or director or someone with whom he or she has a close relationship (a family member or close companion) has a financial or employment relationship with a person who is, or at such time could reasonably be expected to be, a competitor, distributor, agent, customer, or supplier, the employee, officer, or director must disclose this fact in writing to the General Counsel. An employee, officer, or director shall be aware that if he or she enters into a personal relationship with another employee, officer, or director or with an employee, officer, or

director of a competitor, supplier or customer, a conflict of interest might exist that requires full disclosure to the Company. Also, outside employment that adversely affects the performance or interferes with the duties of an employee, officer, or director is a conflict of interest.

An employee, officer, or director shall not, nor shall he or she permit a person having a close personal or business relationship with him or her to offer, solicit nor accept employment or business opportunities for himself or herself or such person based on the Company starting or continuing a business relationship with any supplier, distributor, agent, or customer. The Company also prohibits payment or loan of Company funds or assets to any governmental or political party, candidate, employee, official, etc., for the purpose of supporting or opposing any governmental or political person, entity, or agenda.

1.01.2. Giving and Accepting Business Courtesies

An employee, officer, or director and a person having a close personal or business relationship with him or her may not offer to, nor accept from, any supplier, distributor, agent, customer, or anyone doing business, seeking to do business or competing with the Company an excessive business courtesy. The Company is aware that the definition of “excessive” may vary. An employee, officer, or director shall exercise moderation and good professional judgment in offering or accepting gratuities, including but not limited to gifts, hospitality (including food and drinks) and tickets to cultural, sporting or other special events. Cash is unacceptable in any situation. Any employee in doubt whether a gratuity is acceptable or not, shall seek clarity from his or her supervisor. The general rule of the Company is: If the public disclosure of a business courtesy given or accepted by an employee, officer, or director would be embarrassing to the Company, or to the recipient, the courtesy is inappropriate.

1.01.3. Confidential Information

Cycladic Imports, Inc. prohibits the unauthorized disclosure of confidential or proprietary information about the Company, their customers, suppliers, distributors, agents, or business partners. In carrying out the Company’s business, employees, officers, and directors often learn confidential or proprietary information. The protection of such information is of the highest importance and must be disclosed only with proper authorization. This obligation remains even after the relationship of an employee, officer, or director with the Company ends. Unauthorized disclosure of confidential or proprietary information is illegal and could subject a current or former employee, officer, or director to both criminal and civil liability as well as injunctive relief due to the irreparable harm such disclosure could cause.

Confidential or proprietary information is any information that is not known generally to the public or the industry and includes, but is not limited to, financial and marketing data; operating results; sales; earnings; acquisition targets or potential mergers; acquisition or loss of a major contract; a large financial transaction; major litigation; supplier prices and quotes; distributor, agent or customer inquiries; customer lists and files; price lists, customer sales histories; product information; marketing plans; production costs; personnel files; computer files; process equipment and descriptions; research or business plans; product development; metallurgical codes; formulas and trade secrets.

Proprietary information includes all information obtained by Company employees, officers

and directors during the course of normal work or performance of their responsibilities, regardless of the location.

1.01.4. Fair Dealing

Cycladic Imports, Inc. seeks to outperform its competition fairly and honestly. The Company seeks competitive advantages through superior performance, and never through unethical or illegal business practices. Obtaining or possessing proprietary or trade secret information that was obtained without the owner's consent, or inducing such disclosures by past or present employees of other companies, is prohibited.

1.01.5. Protection and Proper Use of Company Assets

All directors, officers and employees shall endeavor 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 incident of fraud or theft should be immediately reported for investigation. All Company assets shall be used for legitimate business purposes. The use of inside information for personal benefit or disclosure of inside information to others is not only a violation of company policy, but it is also a violation of securities laws that can result in substantial civil and criminal penalties, including fines, penalties and/or imprisonment.

1.01.6. Insider Trading and Tipping

Directors, officers, employees, and agents of Cycladic Imports, Inc. and its subsidiaries shall adhere to the rules and regulations regarding the use and public disclosure of corporate inside information. The purpose of such regulations is to protect the interests of shareholders by providing them with prompt and complete information about significant corporate developments that might affect the value of their investments and to assure that insiders do not profit from information that is not available to the investing public.

Company directors, officers and employees have ethical and legal responsibilities to maintain the confidence of the shareholders of Cycladic, Inc. and the public markets by protecting (as valuable assets) confidential and proprietary information developed by or entrusted to them. Material nonpublic information must not be disclosed to anyone other than persons within the Company whose positions require them to know the information until it has been publicly released. Generally, one may presume that information has been made available to the public two New York Stock Exchange trading days after the formal release of such information.

No director, officer or employee of the Company shall engage in transactions in any securities, whether of Cycladic, Inc., or of any other public companies, while in possession of material nonpublic information regarding such securities, so-called "insider trading." Nor shall any director, officer or employee communicate material nonpublic information to any person who might use such information to purchase or sell securities, so-called "tipping." If there is any doubt whether a particular situation requires refraining from engaging in a securities transaction or sharing information with others, that doubt should be resolved *against* taking that action or the

matter should be discussed with the Company's General Counsel. In addition to these requirements, directors, officers and certain employees, together with family members living in their respective households, are subject to Blackout Periods on trading in Cycladic securities as described under "Blackout Periods."

Generally speaking, any information, whether positive or negative, that a reasonable investor could consider important in deciding whether to buy, sell or hold the securities in question would be "material." Common, but by no means exclusive, examples of "material" information include information concerning sales, earnings, acquisition targets or potential mergers, an important product development, the acquisition or loss of a major contract, a large financing transaction and major litigation. Information that something is likely to happen, or even that it may happen, can be considered material. For example, if someone learns that Cycladic, Inc., is involved in negotiations to make a significant acquisition, even though no agreement has been reached, that person would probably be in possession of material information.

Anyone who is provided with, participates in the preparation of, or otherwise has access to, the monthly financial summary of Cycladic, Inc., or the monthly operating results of the Company or its subsidiaries may be considered to possess material nonpublic information relating to the securities of Cycladic, Inc., until the material information contained in the monthly report has been made public.

The use of inside information for personal benefit or disclosure of inside information to others is not only a violation of company policy, but it is also a violation of securities laws that can result in substantial civil and criminal penalties, including fines, penalties and/or imprisonment.

1.01.7. Blackout Periods

Neither a director or officer of Cycladic Imports, Inc., a director or officer of any of its subsidiaries, any employee of the Company who routinely has access to material nonpublic information (for example, the Company's monthly financial summary), nor any family members living in their respective households, may purchase, sell or otherwise trade in any securities of Cycladic, Inc. during any "Blackout Period."

A "Blackout Period" is that period of time (i) commencing on the first day of the third month of each calendar quarter (e.g., March 1, June 1, September 1 and December 1) and (ii) terminating at the end of the second New York Stock Exchange trading day after the date upon which the Company has released its financial results for such calendar quarter. While Blackout Periods are intended to prevent directors, officers, and the above-described employees and family members from trading in Cycladic's securities at those times when they are most likely in possession of material nonpublic information, such persons shall not engage in transactions in any Cycladic's securities while in possession of material nonpublic information even though such transaction would occur at a time outside any Blackout Period. Additionally, directors, officers and the above-described employees and family members shall pre-clear any transaction involving Cycladic securities through the Company's General Counsel as described under "Pre-clearance and Reporting of Securities Transactions."

1.01.8. Pre-clearance and Reporting of Securities Transactions

Directors, executive officers and 10% stockholders of Cycladic, Inc. must report trading of Cycladic securities in accordance with federal securities laws and regulations. Directors and officers of Cycladic, Inc. and its subsidiaries and employees who routinely have access to material nonpublic information, together with family members living in their respective households, should not engage in any transaction involving Cycladic securities without first obtaining pre-clearance of the transaction from Cycladic General Counsel. When the request for pre-clearance is made, the General Counsel will promptly determine whether the transaction may proceed and, if so, assist the director or executive officer in complying with the reporting requirements of the federal securities laws.

A relatively new rule of the Securities and Exchange Commission permits directors, officers and employees who routinely have access to material nonpublic information to enter into a written plan with their securities broker, at a time when they are not aware of such information, that will govern future purchases or sales of securities (a "Rule 10b5-1 plan"). If the Rule 10b5-1 plan is properly established, purchases or sales may continue under the Rule 10b5-1 plan even during Blackout Periods or periods when the individual is aware of material nonpublic information.

Transactions pursuant to a Rule 10b5-1 plan will not have to be pre-cleared with the General Counsel, but any director, officer or employee wishing to implement a Rule 10b5-1 plan must first pre-clear the plan with the General Counsel. No Rule 10b5-1 plan may be implemented, modified or terminated during a Blackout Period or when the individual is in possession of material nonpublic information. Transactions under a Rule 10b5-1 plan must be reported immediately to the General Counsel so any required Form 4 can be prepared and filed in accordance with applicable federal securities laws. Purchases of stock pursuant to Cycladic's Employee Stock Purchase Plan will not have to be pre-cleared with the General Counsel, but any director or officer of Cycladic Imports, Inc. or any of its subsidiaries or any employee who routinely has access to material nonpublic information may not enroll in that Plan, change the withholding rate or terminate the payroll deduction during a Blackout Period or when the individual is in possession of material nonpublic information.

1.01.9. Business Inquiries

It is important that confidential and certain other kinds of information about the financial or general business status of Cycladic Imports, Inc., and the Company be protected or released under carefully controlled circumstances. Therefore, any comment to inquiries about the Company or the market activity of its stock from reporters, investment analysts or others in the media or the financial community shall be made through an appropriately designated officer. Unless a director, officer, or employee has been expressly authorized to the contrary, he or she shall decline to comment and refer the inquiry to the Public Relations Manager of Cycladic Imports, Inc.

1.01.10. Accounting and Recordkeeping

Financial statements and other financial information shall be accurate, complete and fairly present in all material respects the Company's financial condition and results of operations. All

Company accounting entries shall be true and contain appropriate descriptions of the associated transactions. All Company bank accounts and other accounts and funds shall be reflected on the books or other financial statements of the Company. The Company shall properly disclose certain additional information about its financial condition or operations as required by federal securities laws.

To assure compliance by Cycladic Imports, Inc. with its obligations under federal securities laws,

- Each financial report that contains financial statements, and that is required to be prepared in accordance with (or reconciled to) generally accepted accounting principles and filed with the Securities and Exchange Commission, shall reflect all material correcting adjustments that have been identified by the Company's auditors in accordance with generally accepted accounting principles and the rules and regulations of the Securities and Exchange Commission;
- Each annual and quarterly financial report required to be filed by Cycladic, Inc. with the Securities and Exchange Commission shall disclose all material off-balance sheet transactions, arrangements, obligations (including contingent obligations) and other relationships of Cycladic Imports, Inc. and its affiliates with unconsolidated entities or other persons, that may have a material current or future effect on financial condition, changes in financial condition, results of operations, liquidity, capital expenditures, capital resources or significant components of revenues or expenses; and
- Any pro forma financial information included in any periodic or other report filed by Cycladic, Inc. with the Securities and Exchange Commission or included in any press release, will be presented in a manner that (i) does not contain an untrue statement or omission of a material fact necessary to make the pro forma financial information, in light of the circumstances under which it is presented, not misleading, and (ii) reconciles it with the financial condition and results of operations of Cycladic, Inc. under generally accepted accounting principles.

It is a violation of this code for any employee to participate in an overbilling arrangement with a supplier, distributor, agent, customer or any other person in which the Company issues or accepts an invoice, or receives or makes payment for merchandise, in an amount in excess of the actual price or participate in an underbilling arrangement with a supplier, distributor, agent, customer or any other person in which the Company issues or accepts an invoice, or receives or makes payment for merchandise, in an amount less than the actual price. All records and reports required of and by the Company shall contain true and accurate results.

Any employee who knowingly makes or accepts, or requests an employee to make or accept, false or misleading record entries or reports will be disciplined. The Company shall maintain internal control systems to ensure reliability and adequacy of its records and reports and the Company's ability to record, process, summarize and report financial data. Any fraud and all significant deficiencies in the design or operation of the internal controls must be properly disclosed.

An employee, officer, or director of the Company who has good faith concerns regarding

any questionable accounting or auditing matter with respect to the Company is encouraged to discuss such matter with the principal financial officer of the Company or his or her designee. If the employee, officer, or director wishes, however, he or she may submit his or her concerns regarding any questionable accounting or auditing matter confidentially (and, if he or she so chooses, anonymously) by telephone to the Compliance Line at 800/888-2234 (a toll-free, anonymous, 24 hour, everyday service provided by Global Compliance Services) or by sending a letter marked "Confidential" either to:

Chairman
Audit Committee
Cycladic Imports, Inc.
c/o B.W. Morrison
Jawbright & Fullorski L.L.P.
2200 Ross Avenue, Suite 2800
Houston, Texas 77024-2784
713/855-8301
bmorrison@Jawbright.com

1.01.11. Sales Agent Relationships

All ongoing agency relationships must be formalized through written contracts. Minimally, these contracts shall cover products, territory, compensation, method of payment and duration of the relationship and have the written approval of the President and Chief Executive Officer. Every contract or amendment to an existing contract involving the purchase or sale of products or services in one or more foreign countries shall contain an affirmative representation that all pertinent laws and regulations of the country or countries involved, including the Foreign Corrupt Practices Act, have been and will be complied with fully in connection with such contract.

1.01.12. Ownership of Work Product

Any inventions, improvements, concepts, or ideas made or conceived by a Company employee during his or her employment and related to the business of the Company shall be the sole and exclusive property of the Company. Any work performed by Company employees during the term of employment and any resulting work product shall be considered a "Work Made for Hire" as defined in the U.S. copyright laws, and shall be owned by and for the express benefit of the Company. In the event it should be established that such work does not qualify as Work Made for Hire, each employee must agree to and hereby does assign to the Company all of his or her right, title, and interest in such work product including, but not limited to, all copyrights, patents, trademarks, and other proprietary rights. Employees shall fully cooperate with the Company in the protection and enforcement of any intellectual property rights that may derive as a result of the services performed by employees during the course of employment. This shall include executing, acknowledging, and delivering to the Company all documents or papers that may be necessary to enable the Company to publish or protect such inventions, improvements, concepts, and ideas.

1.01.13. Exceptions and Waivers

An employee must contact his or her appropriate Area Vice President, either directly or

through the employee's supervisor, for guidance in matters that may be outside this code or when such employee is in doubt about the best course of action in a particular situation. Code exceptions shall be reported in writing to the General Counsel (757-233-6170), for resolution and/or approval. Any waiver of this code for executive officers or directors may be made only by the Board of Directors or a Board committee and shall be promptly disclosed as required by law or stock exchange regulation.

1.01.14. Procedures for Reporting any Fraud or Illegal or Unethical Behavior

Each employee is encouraged to report violations of laws, rules, regulations or this Code to his or her supervisor or confidentially (and, if desired, anonymously) by telephone to the Compliance Line at 800/888-2234 or to the General Counsel (757-233-6170) and any Fraud (see definition on page) confidentially (and, if desired, anonymously) by telephone to the Compliance Line at 800/888-2234 or to the Director of Internal Audit of Cycladic, Inc. (757-233-6412). If an employee wishes to report such violations by mail, he or she may write confidentially (and, if desired, anonymously) either the General Counsel or the Director of Internal Audit, as appropriate, at the following address:

Cycladic, Inc.
P. O. Box 803546
Norfolk, VA 23511
Attention: [General Counsel/Director of Internal Audit]

The Company will use reasonable efforts to protect the identity of any employee who reports actual or potential misconduct. It is the policy of the Company not to allow any form of retaliation for (i) reports of misconduct by others made in good faith by employees, including without limitation reports communicated to supervisors, the Compliance Line, the General Counsel, the Director of Internal Audit or governmental officials or (ii) assisting in any investigation of misconduct conducted by a supervisor or other Company representative, any state or federal regulatory or law enforcement agency or any member or committee of the United States Congress. Any person who participates in any retaliation is subject to disciplinary action, including termination. Employees shall not make reports relating to this Code in bad faith or in a false or frivolous manner.

BP 2.01 EQUAL EMPLOYMENT OPPORTUNITY POLICY

Cycladic Imports, Inc. makes all employment and personnel actions in accordance with the laws and principles of equal employment opportunity without regard to race, color, religion, sex, age, sexual orientation, national origin, ADA (*Americans With Disabilities Act*) disability, Workers' Compensation history, military or veteran's status, or other legally protected status. The Company will make reasonable accommodations to allow ADA disabled employees to perform the essential functions of their jobs when such accommodations do not impose an undue hardship on the Company.

This policy covers all phases of employment, including without limitation: recruitment, hiring, assignment, promotion, transfer, layoff, termination, compensation, benefits and training. Participation in company programs (educational, social, recreational, etc.) and use of company facilities are covered also by this policy.

The Company's objective is to provide employees with a working environment free of discrimination, harassment, intimidation or coercion. Employees are expected to treat others with respect and to take positive actions to assure the effectiveness of this policy, both as to the spirit and intent, through continued support, leadership and personal example. The Company prohibits conduct, both verbal and physical, which would violate this policy.

To assure broad communication, Cycladic Imports, Inc. posts this policy at conspicuous locations so all employees and applicants will know of the Company's commitment to equal employment opportunity. Any employee or applicant who wants to discuss concerns regarding this policy should promptly contact the General Counsel (757-233-6170). Employees may contact their supervisor.

BP 3.01 HEALTH & SAFETY POLICY

Cycladic Imports, Inc. is committed to providing a safe office environment where employees are dedicated to an accident-free workplace with maximum possible productivity. Cycladic seeks to achieve its health and safety objectives by:

- Complying with all applicable health and safety laws and regulations.
- Making health and safety considerations an important element in the design, operation and maintenance of its office facilities and the conduct of its business.
- Educating employees regarding their responsibilities for achieving the health and safety objectives of Cycladic Imports, Inc.
- Providing appropriate job skills and safety training.
- Utilizing thorough accident investigation processes that include both prompt incident investigation and root cause analysis tools.
- Communicating openly with employees on occupational health and safety issues.

BP 4.01 SECURITY POLICY

Cycladic Imports, Inc. has a vital interest in protecting its employees, non-employees, their property and the property of the Company. Proper security depends on the cooperation of the entire workforce and is important to the success of the Company. Accordingly, employees and non-employees are expected to comply with this policy, and other general business and personnel policies as well as common sense security practices.

This policy outlines certain security policies and procedures to protect employees and non-employees while on company property. The Company reserves the right to refuse admittance of anyone to company property.

4.01.1. Personal Conduct

Employees are expected at all times to treat each other with courtesy and respect and to conduct themselves in accordance with applicable law and this *Business Policy Manual*. An employee should not be present in the Company's facilities when closed unless he or she is authorized to work at such facilities at that time on behalf of the Company. Employees shall comply with all safety and security instructions, rules, and practices of the Company and governmental authorities, including traffic regulations, while at the Company's facilities or traveling or otherwise working on behalf of the Company. Employees are prohibited from fighting, provoking or instigating a fight or violence involving, or threatening to do bodily harm to, any person at any time at the Company's facilities. Employees shall not engage in horseplay, running, scuffling, throwing objects, or practical jokes that could result in death, personal injury, or property damage. Employees shall at all times cooperate fully with the Company's management and security personnel and with law enforcement officials in connection with any security matter involving the Company's employees or facilities.

4.01.2. Searches

Although employees may be permitted or requested to lock desks, file cabinets, lockers, or other company equipment assigned to them, this company equipment and storage is not intended for the exclusive personal private use of any employee, and the Company retains the full right and ability to have unrestricted access to any such locked equipment at any time. No employee shall expect personal privacy with regard to the use of any such company equipment. Further, no employee shall expect personal privacy of himself or herself or vehicles or containers while on company property.

The Company reserves the right to conduct searches of any employee or non-employee or any company, employee, or non-employee object or item that is on company property when it has sufficient information that there is misconduct related to the Company. Specifically, but not limited to, the Company is authorized to search work areas, lockers, desks, purses, briefcases, baggage, lunch containers, and clothing on company property. The Company also reserves the right to conduct searches on its property with or without the employee being present and with or

without notice. Such searches shall have the prior approval of the General Counsel.

The Company reserves the right to conduct non-investigatory searches in the employee's workplace (*e.g.*, such as going into an employee's desk or file cabinet to get materials or information needed for usual business purposes) when the employee is unavailable.

4.01.3. Weapons

The Company prohibits all persons (except authorized security personnel) from carrying a handgun, firearm, or prohibited weapon of any kind onto company property regardless of whether the person is licensed to carry the weapon or not. Prohibited weapons include any form of weapon or explosive that has the potential to inflict harm or is restricted under local, state or federal law or regulation. This policy applies to all employees, and to non-employees on company property, except authorized security personnel.

The Company recognizes the law allows citizens who meet certain requirements to carry a concealed handgun; however, company policy prohibits firearms on company property, including firearms carried under a concealed handgun license.

BP 5.01 COMPUTER & COMMUNICATION SYSTEMS POLICY

5.01.1 General

Cycladic Imports, Inc. owns and operates a variety of computer and communication systems that are provided for its employees to use to conduct company business. These systems which include computer, electronic mail (e-mail), Internet, Intranet, public address, radio, telephone, cellular phone, pager, facsimile and voice mail equipment and services have become prevalent tools for business communications and information management. Access to company computer and communication systems and equipment is a privilege, not a right. Employees are expected to use them in an effective, efficient, ethical and lawful manner. The same standards of business conduct expressed in other company policies are applicable to the conduct of business when using company computer and communication systems and equipment.

Employees shall take precautions to protect computer and communication systems and equipment from theft or misuse. Employees are prohibited from accessing or using computer and communication systems and equipment without authorization; altering data in a computer without authorization; transmitting computer viruses or conducting any other activity intended to negatively affect the operation of any company or outside computer, computer system or communication system. All material transmitted by a company computer or communication system shall correctly identify the transmitter of the material.

All information and data files contained in computer and communication systems and equipment are valuable assets of Cycladic. Access to the Cycladic's computer and communication systems are assigned and managed by Cycladic. Users may not transfer or confer any of these privileges to another individual.

As with all company assets, the Company's equipment and data exist solely for the benefit of the Company and are not intended to be utilized for the benefit of any individual. E-mail, voice mail and electronic data are intended for authorized business use only. The Company must have full and unrestricted access to all information stored within its electronic systems. This may include retrieving business information, troubleshooting hardware and software, preventing system misuse, monitoring (including logging and reporting) usage and complying with licensing agreements, contracts and regulations. Thus, all information stored within any company electronic system is subject to review at anytime, and no such information can be considered private. No employee has an expectation of personal privacy with regard to any such information.

Who is Affected: This policy affects all employees of Cycladic and its subsidiaries, and all suppliers which include contractors, consultants, business partners, and others granted access to Cycladic computer and communications systems. All individuals who deliberately violate these policy or procedures will be subject disciplinary action up to and including termination and other legal actions as deemed appropriate by the General Counsel.

5.01.2. Computer and Communications Systems Security

Only authorized users are granted access to information systems, and users are limited to specific defined, documented and approved applications, levels of access rights, and space facility access. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability. Employees are prohibited from gaining access to company systems by using another employees password or IDs.

5.01.2.1. Affected Systems and Spaces

This policy applies to all computer, communication systems, and computing spaces owned or operated by Cycladic and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

5.01.2.2. Physical Access

All information processing areas used to house computer resources supporting mission critical applications must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations. Physical access to these areas shall be restricted to authorized personnel.

- Physical access to Cycladic centrally administered computer facilities is restricted to individuals having prior authorization from the IT Manager and displaying at all times while on Company property, an authorized security badge. Authorized visitors shall be supervised, accompanied and logged into a log book (see Appendix C).
- The responsibility for securing the Company's administered computer facilities and/or equipment from unauthorized physical access and/or improper use rests with the appropriate shift manager.

5.01.2.3. Entity Authentication

Any User (remote or internal), accessing Cycladic networks and systems, must be authenticated. The level of authentication must be appropriate to the data classification and transport medium. Entity authentication includes but is not limited to:

- An unique user identifier
- At least one of the following
 - ◆ Biometric identification
 - ◆ Password (see password policy)
 - ◆ Personal identification number
 - ◆ A telephone callback procedure
 - ◆ Token
- Automatic logoff

5.01.2.4. Workstation Access Control System

All workstations used for this Cycladic business activity, no matter where they are located, must use an access control system approved by Cycladic. Systems should require a valid Cycladic login

account, and in particular there will be no “default accounts” or automatic login of systems. In most cases this will also involve password-enabled screen-savers with a time-out-after-no-activity feature. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all applications and networks. Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 30 minutes). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized users absence.

5.01.2.5. Disclosure Notice

A notice warning that those should only access the system with proper authority will be displayed initially before signing on to the system. The warning message will make clear that the system is a private network or application and those unauthorized users should disconnect or log off immediately.

5.01.2.6. System Access Controls

Access controls will be applied to all computer-resident information based on its Data Classification to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

5.01.2.7. Access Approval

System access will not be granted to any user without appropriate approval. Management is to immediately notify the IT Manager and report all significant changes in end-user duties or employment status. User access is to be immediately revoked if the individual has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job.

5.01.2.8. Limiting User Access

Cycladic approved access controls, such as user logon scripts, menus, session managers and other access controls will be used to limit user access to only those network applications and functions for which they have been authorized. Specifically, corporate intranet, Internet, email authorizations will be tailored to each individual job requirements and responsibilities. Firewalls will monitor all activities within sensitive corporate activities and all activities requiring access to Internet sites and email outside the corporate intranet.

5.01.2.9. Need-to-Know

Users will be granted access to information on a need-to know basis. That is, users will only receive access to the minimum applications and privileges required for performing their jobs.

5.01.2.10 Compliance Statements

Users who access to this Cycladic's information systems must sign a compliance statement prior to

issuance of a user-ID. A signature on this compliance statement indicates the user understands and agrees to abide by these Cycladic policies and procedures related to computers and information systems. Annual confirmations will be required of all system users.

5.01.2.11 Audit Trails and Logging

Logging and audit trails are based on the Data Classification of the systems.

5.01.2.12 Confidential Systems

Access to confidential systems will be logged and audited in a manner that allows the following information to be deduced:

- Access time
- User account
- Method of access
- All privileged commands must be traceable to specific user accounts

In addition logs of all inbound access into Cycladic's internal network by systems outside of its defined network perimeter must be maintained. Audit trails for confidential systems should be backed up and stored in accordance with Cycladic back-up and disaster recovery plans. All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. All logs must be audited on a periodic basis. Audit results should be included in periodic management reports.

5.01.2.13 Access for Non-Employees

Individuals who are not employees, contractors, consultants, or business partners must not be granted a user-ID or otherwise be given privileges to use the Cycladic computers or information systems unless the written approval of the Department Head has first been obtained. Before any third party or business partner is given access to this Cycladic computers or information systems, a chain of trust agreement defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization.

5.01.2.14 Unauthorized Access

Employees are prohibited from gaining unauthorized access to any other information systems or in any way damaging, altering, or disrupting the operations of these systems. System privileges allowing the modification of production data must be restricted to production applications.

5.01.2.15 Remote Access

This remote access policy defines standards for connecting to the Cycladic organizational network and security standards for computers that are allowed to connect to the organizational network.

This remote access policy specifies how remote users can connect to the main organizational network and the requirements for each of their systems before they are allowed to connect. This will specify:

1. The anti-virus program remote users must use and how often it must be updated.
2. What personal firewalls they are required to run.
3. Other protection against spyware or other malware.

The remote access policy defines the methods users can use to connect remotely such as dial up or VPN. It will specify how the dial up will work such as whether the system will call the remote user back, and the authentication method. If using VPN, the VPN protocols used will be defined. Methods to deal with attacks should be considered in the design of the VPN system.

5.01.2.15.1. Purpose

This remote access policy is designed to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data.

5.01.2.15.2. Approval

Any remote access using either dial-in, VPN, or any other remote access to the organizational network must be reviewed and approved by the appropriate supervisor. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

5.01.2.15.3. Remote Computer Requirements

1. The anti-virus product called McAfee VirusScan Enterprise 8.0i is required to be operating on the computer at all times in real time protection mode.
 - a) The anti-virus product shall be operated in real time on the computer. The product shall be configured for real time protection.
 - b) The anti-virus library definitions shall be updated at least once per day.
 - c) Anti-virus scans shall be done a minimum of once per week.
 - d) No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.
2. The computer must be protected by a firewall at all times when it is connected to the Internet. Popular choices include Zone Alarm, the Windows XP firewall, and Norton Personal firewall.

5.01.2.15.4. Remote Connection Requirements

The remote user shall use either dial-In or virtual private networking (VPN). Dial-In is typically used when the user is in a local calling area and a high-speed connection is not available. VPN is typically used when the user would need to dial a long distance number to connect with a dial-in connection, or when a high speed (broadband) network connection is being used. VPN creates a protected tunnel to the organizational network, and is generally preferred over dial-in. This section specifies the requirements for Dial-In and VPN connections.

5.01.2.15.5. Dial-In Requirements

1. Number check - The dial in settings shall be set to perform one or the other of:
 - a) Verify Caller ID to a specific number - Use this option if caller ID is available
 - b) Always Call back to a specific number - If the user must connect from a location other than their designated location such as their home, they should use VPN.
2. Client Check - A requirement that must be set for Dial-In clients is that a firewall must be installed and operational. If the Dial-In client does not meet the criteria, either the connection is not allowed or the client can only access a limited area where they can get the software needed to meet the requirement.
3. Authentication - For authentication of the user, the dial in connection shall use one of:
 - a) MS-CHAP version 2
 - b) EAP-RADIUS
 - c) EAP-TLS
 - d) EAP-MD5-Challenge
4. Connection Encryption – Encryption should always be used if it is available. If a situation arises where a remote user cannot use an encrypted connection, then that user should not access or attempt to access confidential information. Encrypted connections shall use one of the following encryption mechanisms:
 - a) Microsoft Point to Point Encryption (MPPE)
 - b) IPSec

5.01.2.15.6. VPN Requirements

1. Client Check - A requirement that must be set for VPN clients is that a firewall must be installed and operational. Also Anti-virus software must be installed and operational. If the VPN client does not meet the criteria, either the connection is not allowed or the client can only access a limited area where they can get the software needed to meet the requirement.
2. The connection choices are PPTP, L2TP, IPSec, and SSL. The connection shall use IPSec set to encrypt the data sent through the connection.
3. Authentication - For authentication of the user, the VPN connection shall use Internet Key Exchange (IKE) with digital certificates. The other choice is Internet Key Exchange (IKE) with a preshared key.

5.01.3. Passwords

To gain access to Cycladic information systems, authorized users, as a means of authentication/access control must supply individual user passwords. These passwords must conform to certain rules contained in this document. The confidentiality and integrity of data stored on company computer systems must be protected to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employees job duties.

5.01.3.1. Affected Systems

This policy applies to all computer and communication systems owned or operated by Cycladic and its subsidiaries. Similarly, this policy applies to all platforms (operating systems) and all application systems.

5.01.3.2. User Authentication

All systems will require a valid user ID and password. All unnecessary operating system or application user IDs not assigned to an individual user will be deleted or disabled.

5.01.3.3. Password Storage

Passwords will not be stored in readable form without access control or in locations where unauthorized persons might discover them. All such passwords are to be strictly controlled using either physical security or computer security controls.

5.01.3.4. Application Passwords Required

All programs, including third party purchased software and applications developed internally by Cycladic must be password protected.

5.01.3.5. Choosing Passwords

All user-chosen passwords must contain at least one alphabetic, one non alphabetic character, and a minimum of eight non-blank characters. The use of control characters and other non-printing characters are prohibited. All users must be automatically forced to change their passwords appropriate to the classification level of information. To obtain a new password, a user must present suitable identification.

Additional suggestions for password selection are listed below:

- Password does not include the users own or, to the best of his/her knowledge, close friends - or relatives - names, employee number, Social Security number, birth date, phone number, company id-number, for any information about him/her that the user believes could be readily learned or guessed.
- Password does not, to the best of the users knowledge, include common words that would

be in an English dictionary, or from another language with which the user has familiarity.

- Password does not, to the best of the users knowledge, employ commonly used proper names, including the name of any fictional character or place.
- Password does not contain any simple pattern of letters or numbers, such as qwertyxx or xyz123.

5.01.3.6. Changing Passwords

All passwords must be promptly changed, typically within 1 business day, if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties. All users must be forced to change their passwords at least once every sixty (60) days.

5.01.3.7. Sharing Passwords

Individuals must not share passwords. The only exception is in emergency circumstances or when there is an overriding operational necessity. Prior agreement from the Computer Center Security officer is required before sharing passwords. The owner of this account must change his/her password as soon as possible, typically within 1 business day after a password has been compromised or on direction from management.

5.01.3.8. Password Constraints

The display and printing of passwords should be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three unsuccessful attempts to enter a password, the involved user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three minutes, or (c) if dial-up or other external network connections are involved, disconnected.

5.01.3.9. Transmitting Passwords

Passwords should never be transmitted in the clear (unencrypted), and no applications should be used which transmit passwords in the clear. In special circumstances this requirement may be waived, but there must be a clear need and written authorization must be obtained from the Compliance Office.

5.01.4. Data Protection and Encryption Policy

5.01.4.1. Protection of Data on Portable Devices

Any portable device which leaves Cycladic property, including laptops, disks, USB storage devices, and similar items, must have data stored in an encrypted form so that physical access to the device does not reveal private information.

5.01.4.2. Protection of Sensitive Data on Cycladic Equipment

Encryption provides additional protection against compromise of sensitive information, and

employees are encouraged to use encryption for particularly sensitive data even when stored on Cycladic equipment. In particular, any reports or spreadsheets generated that include private personal information, such as social security numbers or bank account numbers, should be encrypted.

5.01.4.3. Key Escrow

Data protected using encryption is a valuable asset to Cycladic, and recovery of such data must be possible. Therefore, any employee using encryption to protect company information must provide a copy of the key/password/passphrase to the Office of Compliance for safekeeping. Form KE-1 in Appendix D should be used for this purpose. The Office of Compliance shall protect such information with effective physical measures, such as keeping the key information in a locked safe.

5.01.5. Network Scanning Policy

5.01.5.1. Network Scan Types and Scope

This network scanning policy defines network scan types, identifies reasons for scanning, identifies times when network scanning is allowed, who should approve network scanning, and specifies who should be notified when network scanning is done.

1. Network device location scan - This scan may use different means to determine IP addresses of active devices on the network. Methods:
 - a) ARP Scan - An ARP broadcast can be sent to network IP addresses asking what is the MAC address of the host with IP address x.x.x.x. If a response occurs, there is an active host at that address.
2. Internal full port scan - Checks to determine what services are running on each host. This may be done against selected hosts or all hosts including servers and workstations. Methods:
 - a) Connect scan - Tries to complete a connection to a port on a host computer. This scan allows the host computer to log the connection.
 - b) SYN scan - Sends a SYN packet to the host indicating that it wants to open a socket. But when the host responds it does not finish establishing the connection.
 - c) FIN scan - Sends a FIN packet to a host port. If a service is not running, the port responds with a reset signal. If the port has a service running on it, the signal is ignored.
3. External full port scan - Checks to determine what services are running on each host. This test is done from outside the firewall and is directed toward any IP addresses owned by the organization being tested. It may use the socket connect scan method, the SYN scan method, or the FIN scan method.
4. Internal vulnerability scan - Tests the server to see if it is vulnerable to known flaws in the operating system, services, and applications that are running. This test may be directed toward one or more hosts including servers and workstations. This test goes beyond performing a full port scan. It attempts to get information about the operating system and services running on the host. It will attempt to determine the version of the services running

on the host, and may do a penetration test.

5. External vulnerability scan - Same as the internal vulnerability scan except it is done from outside the organization network and is directed toward any IP address owned by the organization being tested.
6. Internal denial of service scan - This is a scan using packets which are intentionally designed to make a system crash or tie up resources. The scan is directed against ports but the data sent is usually mis-configured in some unusual way.
7. External denial of service scan - Similar to the internal denial of service scan except it is directed against IP addresses owned by the organization being tested.
8. Password Cracking - This test may send default passwords and brute force password guessing against accounts on specified systems. This is really not a network scan but is covered in this policy since it could potentially disrupt service depending on the password policies of the organization.

Many scanning services will offer some combinations of these types of scans. This policy covers all types of network and host scanning.

5.01.5.2. Network Scanning Reason

Network scanning may be performed for several reasons

1. To determine whether computer systems are vulnerable to attack and fix them.
2. To show companies we interact with that our servers are reasonably secure.
3. To fulfill regulatory requirements.

Network scanning shall not be performed without written permission.

5.01.5.3. Network Scanning Disruptions

Network scanning can be very disruptive to both a network and hosts that are operating on a network. No network scanning shall be allowed without close adherence to this policy and the associated procedures. Network scanning can cause systems to crash and network devices to become unreliable which can become very disruptive to the business operations.

5.01.5.4. Authorizers of Network Scanning and allowable hours

The head of the IT department shall determine who is authorized to perform network scans. Those who perform network scans must have authorization in writing and a specified time period when they are permitted to perform network scans. This policy may limit the hours that scanning may be done so scanning is not done during business hours. Typically this would mean that scans should occur between 6:00PM and 7:00AM or on weekends when no business critical tasks are planned.

5.01.5.5 Scanning Notifications

When scanning is to be done, the following groups of people must be notified on a daily basis:

1. The IT manager

2. The manager responsible for system administration of the computer system to be scanned.
3. The manager of applications running on the computer system to be scanned.
4. The users of computer systems that will be scanned.

5.01.5.6. Scanning Procedure

A scanning procedure shall be created for all computer systems to be scanned. For each server to be scanned a list of people to be notified shall be maintained. For workstations to be scanned, users may be notified using a group email.

5.01.5.7. Denial of Service Scan

Denial of service scan shall not be done without signoff of both the head of IT and Cycladic CEO. This is due to the fact that denial of service scans are an effort to disrupt service and will most likely disrupt one or more services. It may cause key network devices to fail. The hours during which a denial of service scan may be done shall be strictly limited and normally only after normal business hours.

5.01.5.8. Enforcement

Since network scanning can be disruptive to the operations of the network and the organization, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

5.01.6. Wireless Communication

Cycladic Imports, Inc. prohibits access to its networks via unsecured wireless communication mechanisms or devices. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the Security Administrator are approved for connectivity to Cycladic's networks.

5.01.6.1. Scope

This policy covers all wireless data communication devices (e.g., laptop computers, cellular phones, PDAs, etc.) connected to any of Cycladic's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Cycladic's networks do not fall under the purview of this policy.

5.01.6.2. Register Access Points and Cards

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by the IT Manager. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with the IT Manager.

5.01.6.3. Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations (contact the IT Manager for a current list).

5.01.6.4. VPN Encryption and Authentication

All personal computers/laptop computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point encryption using keys of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database.

5.01.6.5. Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

5.01.6.6. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.01.7. Virus Protection

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software. This policy defines anti-virus policy for every Cycladic computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of file attachments are blocked at the mail server and what anti-virus program will be run on the mail server.

5.01.7.1. Information Technology Responsibilities

IT shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

5.01.7.2. Employee Responsibilities

Employees shall:

1. Not knowingly introduce a computer virus.
2. Employees shall not load storage devices (e.g., floppy or compact disks, or USB storage devices), files, e-mail attachments and software of unknown origin.
3. Incoming storage devices shall be scanned for viruses before they are used in company

computers.

4. Any associate who suspects that his/her workstation has been infected should POWER OFF the workstation and call the IT manager.

5.01.7.3. Anti-Virus Software

The organization will use a single anti-virus product for anti-virus protection and that product is McAfee VirusScan Enterprise 8.0i. The following minimum requirements shall remain in force.

1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
2. The anti-virus library definitions shall be updated at least once per day.
3. Anti-virus scans shall be done a minimum of once per week on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

5.01.7.4. Email Server & Malware

The email server will have additional protection against malware since email with malware must be prevented from entering the network.

5.01.7.5. Email Malware Scanning

In addition to having the standard anti-virus program, the email server or proxy server will additionally scan all email for viruses and/or malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

5.01.7.6 Blocked Attachment Types

The email server or proxy server will block all emails with attachment types listed in Appendix B. This is because these attachment types are dangerous containing active content which may be used to infect a computer with hostile software or because these attachment types are commonly successfully used by virus programs or malware to spread.

5.01.8. Spyware

Spyware and adware can compromise system performance and allow sensitive information to be

transmitted outside the organization. Spyware installation programs can launch even when users are performing legitimate operations, such as installing a company-approved application. As a result, combating spyware requires user vigilance as well as IT management and control.

5.01.8.1. IT Responsibilities

IT personnel will do the following:

1. Install and update appropriate anti-spyware software on all computers.
2. Respond to all reports of spyware installation, remove spyware modules, restore system functionality, and document each incident.

5.01.8.2. Employee Responsibilities

The following applies:

1. Employees shall not knowingly allow spyware to install on company computers.
2. Employees shall perform anti-spyware updates and run anti-spyware programs regularly, as directed by the IT department.
3. Employees shall immediately report any symptoms that suggest spyware may have been installed on their computer.

5.01.9. Server Documentation Policy

5.01.9.1. Overview

This policy is an internal IT policy and defines the requirements for server documentation. It is designed both to protect the organization against loss of service by providing minimum requirements for monitoring servers. It also provides for monitoring servers for file space and performance issues.

The policy also defines the level of server documentation required such as configuration information and services that are running, who will have access to read server documentation and who will have access to change it. It also defines who will be notified when changes are made to the servers.

5.01.9.2. Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy complements Cycladic's disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to any servers.

5.01.9.3. Documentation

5.01.9.3.1 Performance Documentation

All production servers and infrastructure support servers including but not limited to the following types of servers shall be documented daily:

1. File servers
2. Database servers
3. Mail servers
4. Web servers
5. Application servers
6. Domain controllers
7. FTP servers
8. DNS servers

5.01.9.3.2 Daily Checking

All servers shall be checked manually on a daily basis by 9:30AM the following items shall be checked and recorded:

1. The amount of free space on each drive shall be recorded in a server log.
2. The system log shall be checked and any major errors shall be checked and recorded in the server log.
3. Services shall be checked to determine whether any services have failed.
4. The status of backup of files or system information for the server shall be checked daily.

5.01.9.3.3. External Checks

Essential servers shall be checked using either a separate computer from the ones being monitored or a server monitoring service. The external monitoring service shall have the ability to notify multiple IP personnel when a service is found to have failed. Servers to be monitored externally include:

1. The mail server
2. The web server
3. External DNS servers
4. Externally used application servers.
5. Database or file servers supporting externally used application servers or web servers.

5.01.9.3.4. Documentation

For every server on the Cycladic network, a number of items must be documented and reviewed on a regular basis to keep it private and secure. This list of information about every server should be created as servers are added to the network and updated regularly.

1. Server name
2. Server location
3. The function or purpose of the server.

4. Hardware components of the system including the make and model of each part of the system.
5. List of software running on the server including operating system, programs, and services running on the server.
6. Configuration information about how the server is configured including:
 1. Event logging settings
 2. A comprehensive list of services that are running.
 3. Configuration of any security lockdown tool or setting
 4. Account settings
 5. Configuration and settings of software running on the server.
7. Types of data stored on the server.
8. The owners of the data stored on the server.
9. The sensitivity of data stored on the server.
10. Data on the server that should be backed up along with its location.
11. Users or groups with access to data stored on the server.
12. Administrators on the server with a list of rights of each administrator.
13. The authentication process and protocols used for authentication for users of data on the server.
14. The authentication process and protocols used for authentication for administrators on the server.
15. Data encryption requirements.
16. Authentication encryption requirements.
17. List of users accessing data from remote locations and type of media they access data through such as Internet or private network.
18. List of administrators administrating the server from remote locations and type of media they access the server through such as Internet or private network.
19. Intrusion detection and prevention method used on the server.
20. Latest patch to operating system and each service running.
21. Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.
22. Emergency recovery disk and date of last update.
23. Disaster recovery plan and location of backup data.

5.01.9.4. Mail Server Documentation

The following items regarding the Company mail server should be documented:

1. Account size limit where the person receives warnings about mailbox size.
2. Account size limit where the person cannot send mail anymore.
3. Account size limit where the person cannot receive mail anymore.

5.01.9.5. Access

Cycladic IT server administration staff and their management shall have full read and change access to server documentation for the server or servers they are tasked with administering. The IT networking staff, enterprise security staff, application development staff, and help desk staff shall have the ability to read all server documentation.

5.01.9.6. Change Notification

The network administration staff, application developer staff, and IT management shall be notified when changes are made to servers. Notification shall be through email to designated groups of people.

5.01.9.7. Documentation Review

The network or IT manager shall ensure that server documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any server changes were made. Also any current or completed projects affecting server settings should be reviewed to determine whether there were any server changes made to support the project.

5.01.9.8. Storage Locations

Server documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help construct the IT infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

5.01.10. Data Backup

This policy defines the backup policy for computers within the organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server. This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

5.01.10.1. Scope

This policy applies to all equipment and data owned and operated by the organization.

5.01.10.2. Definitions

1. Backup - The saving of files onto magnetic tape or other offline mass storage media for the

purpose of preventing loss of data in the event of equipment failure or destruction.

2. Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
3. Restore - The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

5.01.10.3. Timing

Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

5.01.10.4. DAT Tape Storage

There shall be a separate or set of DAT tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday. There shall be a separate or set of tapes for each Friday of the month such as Friday1, Friday2, etc. Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday. Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.

5.01.10.5. Tape Drive Cleaning

DAT tape drives shall be cleaned weekly and the cleaning tape shall be changed monthly.

5.01.10.6. Monthly Backup

Every month a monthly backup tape shall be made using the oldest backup tape or tape set from the tape sets.

5.01.10.7. Age of tapes

The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than six months shall be discarded and replaced with new tapes.

5.01.10.8. Responsibility

The IT department manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

5.01.10.9. Testing

The ability to restore data from backups shall be tested at least once per month.

5.01.10.10. Data Backed Up

Data to be backed up include the following information

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems required to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. Test database server
7. Test web server

5.01.10.11. Archives

Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

5.01.10.12. Restoration

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

5.01.10.13. Tape Storage Locations

Offline tapes used for nightly backup shall be stored in an adjacent building in a fireproof safe. Monthly tapes shall be stored across town in our other facility in a fireproof safe.

5.01.11. Disaster Recovery Policy

5.01.11.1. Purpose and Objectives

This policy defines and clarifies policies, principles, standards, guidelines, and responsibilities related to the security of the Cycladic's information technology resources and the disaster recovery plan for which it outlines. Disaster recovery's primary objectives are:

- To reduce the risk of disruption of operations or loss of information;
- To communicate responsibilities for the protection of information and continuity of operations;
- To establish a plan for restoration of information and operations following a disaster.

5.01.11.2. Disaster Recovery Policy

Cycladic's disaster recovery plan will attempt to identify and militate against risks to critical

systems and sensitive information in the event of a disaster. The plan shall provide for contingencies to restore information and systems if a disaster occurs. The concept of disaster recovery assumes rapid as feasible resumption of business functions and operations.

Disaster recovery plans must serve several core principles. These include

- Information is an asset which has value to the organization and needs to be suitably protected.
- Information resources must be available when needed.
- Continuity of information resources supporting critical services must be ensured in the event of a disruption to business or a disaster, which makes critical systems unavailable.
- Risks to information resources must be managed.
- The expense of security safeguards must be cost effective and commensurate with the value of the assets being protected.

5.01.11.3. Standards

Cycladic's disaster recovery plans must include the following elements (also see appendix E):

- Business impact analysis, including risk assessment, asset classification, and potential disruption to stakeholders.
- Classification system to identify critical systems and essential records;
- Mitigation strategies and safeguards to avoid disasters. Safeguards should include protective measures such as redundancy, fire suppression, uninterruptible power supply (UPS), surge protection, and environmental measures to protect sensitive equipment from dust, temperature or humidity.
- Backups and offsite storage.
- Business resumption.
- Contingency plans for different types of disruption to information systems.
- Organizational responsibilities for implementing the disaster recovery plan.
- Procedures for reporting incidents and implementing the disaster recovery plan and escalating the agency or institution's response to a disaster.
- Multiple site storage of back-up documents identified in the plan.
- Training, testing, and improvement.
- Annual review and revision.

5.01.11.4. Development Responsibility

The IT Manager is accountable for the disaster recovery plan.

5.01.12. Employee Termination or Retirement

An employee's employment status or work location can compromise the provisions of the Company's security policy. In cases of termination or retirement, specific processes must be

implemented to maintain the integrity of the Company's information system.

5.01.12.1. Supervisors Responsibility

Managers and supervisors should notify the IT manager and the Human Resources Department promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

5.01.12.2. Human Resources Responsibility

The human resources department will provide an updated corporate headquarters employee roster. Dated updates will be promulgated within a week of any change. Human Resources will notify the IT department upon associate transfers, retirements or terminations. Involuntary terminations must be reported prior to the termination.

5.01.13. Privacy

Employees shall respect the privacy of other employees regardless of whether their computer and communication system or equipment is securely protected. Ability to access another employee's computer or communication system, equipment or accounts does not, by itself, imply authorization to do so. Viewing or printing the files of others without a specific Company related business purpose for doing so may result in disciplinary action, up to and including termination. Further, dissemination of confidential or internal Company information, including Company forms, policies, procedures and communications, or confidential third-party information, to anyone outside the Company, except for legitimate Company business purposes, is prohibited. This policy includes, but is not limited to, documents, e-mail, on-line information on the Company's internal network or elsewhere, voice mail, calendars and databases or their associated reports.

5.01.14. Copyright

The Company's policy is to strictly comply with copyright law with respect to the copying of documents. The current federal copyright law (Title 17 U.S. Code) governs the making of photocopies and/or other reproductions of copyrighted materials by individuals.

Under the recent copyright law amendments dictated by the Berne Convention, a copyright owner no longer has to include a copyright notice on his or her work for it to be protected by a copyright. Any original work of authorship, whether published or unpublished, created in tangible form subsequent to March 1, 1989, is automatically afforded copyright protection.

Sections 106, 107 and 108 of the copyright law dictate the rights of copyright owners and under what circumstances a photocopy of a copyrighted work may legally be made. To this end, appropriate copyright notice signs will remain posted near each of our photocopy machines, both attended and unattended.

Any information (including text, software, graphics and photographs) that is copyrighted, shall not be copied into, from, by or placed on any company computer, except in accordance with licensing agreements and written approvals. Employees are expected to honor federal copyright laws that protect commercial software. Use of software under any condition that does not meet the terms of

the software licensing agreement is prohibited. Duplicating, transmitting or using software not in compliance with software license agreements is considered copyright infringement.

5.01.14.1. Civil Penalties

Violations of copyright law expose the company and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to \$100,000 for each illegal copy

5.01.14.2. Criminal Penalties

Violations of copyright law that are committed willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b)), expose the company and the employee(s) responsible to the following criminal penalties:

- Fines up to \$250,000 for each illegal copy
- Jail terms of up to five years

5.01.15. Confidentiality

Information regarding company computer and communications equipment and systems and certain computer files and data created by employees may be considered confidential information.

Employees who manage confidential information on their computers shall use passwords and other precautions to protect such information. The protection of confidential information is covered by the Business Conduct Policy. Copying data and files from company systems without the written consent of the appropriate department manager is a breach of confidentiality.

5.01.16. Hardware and Software Acquisition and Use

The Company has established standard software and hardware for commonly used applications. Purchases of computer and communication system equipment and software shall have proper review and approval and be in accordance with all company procedures.

The Company's policy is to strictly observe the copyrights on computer software. Under federal copyright law, the Company can duplicate copyrighted software only in specific conformance with individual software license agreements; any violation of these agreements can subject the Company to substantial penalties. The following guidelines should be adhered to strictly by all personnel of the Company:

1. The Company licenses the use of computer software from a variety of outside companies. The Company does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.
2. Company personnel must use any licensed software strictly in accordance with individual licenses. This specifically includes copying Company-licensed software for home use.

3. No new software or additional copies of existing software will be installed on Company computers without the consent of the IT Manager or his designated representative as responsible for information systems. This consent is required for both personally-licensed and Company-licensed software.
4. The Company must account for all software installed on its computers, whether personally or Company-licensed. A copy of company purchased/authorized software is found in Appendix A.
5. Company personnel learning of any misuse of software or related documentation within the Company shall notify the Company's General Counsel.
6. According to federal copyright law, illegal reproduction of software can result in civil damages of as much as \$100,000 per occurrence, as well as criminal penalties including fines and imprisonment. Company personnel who make, acquire or use unauthorized copies of computer software and documentation will be dealt with as appropriate under the circumstances, which may include termination.
7. Only the centralized Information Technology organizations in the company are authorized to maintain, to download and/or install from installation media software for use at Cycladic.

Computers, computer-related equipment (printers, modems, etc.), radios, telephones, cellular phones, pagers, facsimiles and other communication equipment no longer in use are to be turned in immediately to the appropriate controlling department by department managers. Requests for such used equipment may be made in writing.

5.01.17. Unauthorized Uses

Use of company computer and communication equipment and systems for fraudulent, harassing, indecent, profane, intimidating or other unlawful uses is prohibited. Specifically, but without limitation, transmission of files, messages or images that may constitute intimidating, hostile or offensive material on the basis of sex, race, color, religion, national origin or disability is prohibited.

Company computers and communication equipment and systems are not to be used for personal entertainment or any other purpose prohibited by this or any other company policies.

Employees are not authorized to use company computer and communication equipment and systems for commercial activities, religious causes, charitable solicitations, political activity, support for outside organizations, or other activities, which are not related to the direct conduct of company business. Commercial activities include conducting business as an agent or owner of either a business or non-profit organization or any advertising of personal services or products.

5.01.18. Electronic Mail & Internet User Guidelines

Many of Cycladic's computers provide access to the Company's internal network and outside networks, both public and private, which furnish information, messages, electronic mail, news, etc. Access is permitted through the Company-wide system or a local provider with prior approval of

the IT Division manager.

All outgoing messages that do not reflect the official position of the Company should clearly state that fact (e.g., include a disclaimer, such as “The opinions expressed here are my own and do not necessarily represent those of Cycladic Imports, Inc.”). Employees should be aware that when transmitting confidential and/or sensitive information via e-mail, privacy and confidentiality cannot be guaranteed. All messages should be composed with the expectation that they could be made public. Employees shall identify themselves clearly and accurately in all electronic communications and be aware that it is unethical to alter the source or message of any e-mail. Employees are prohibited from sending junk mail and chain letters.

Employees are expected to manage their company mail folders in accordance with the current email retention policy. Except under the circumstances described in the next paragraph, e-mail that is over 90 days should be deleted and not retained unless there is a valid business reason.

The Company's e-mail system is not designed to be an effective and reliable system for long term maintenance of business documents. Important business information and files shall be retained using established procedures. Various laws, regulations and orders prohibit the destruction of e-mails (as well as other records, documents and objects) in contemplation of, or during the pendency of, any lawsuit, proceeding, governmental investigation, bankruptcy, or other specified circumstances involving the Company.

Any employee who knows of such circumstances should immediately (i) cease any destruction of relevant e-mails and (ii) advise the General Counsel, who will coordinate with the appropriate information services personnel to implement procedures for the retention of relevant e-mails.

Employees are trusted and expected to exercise good judgment in both duration and frequency of Internet use and to access Internet sites for job-related purposes only. Employees are prohibited from intentionally accessing or forwarding sites that are considered offensive or objectionable in nature or content. Employees are not permitted to access entertainment and pornographic sites, or to view, download, or use any other method to retrieve any related files or programs.

5.01.18.1. Monitoring

All messages created, sent, or retrieved over the Internet are the property of the Company and may be regarded as public information. Cycladic reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.

5.01.18.2. Employee Responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employees name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable company policies dealing with security and confidentiality of company records.
5. Run a virus scan on any executable file(s) received through the Internet. (Note: specific files are currently blocked (see paragraph 5.01.7.6)
6. Avoid transmission of nonpublic customer information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.
7. Shall not install Instant messaging (IM) client software, e.g. AOL AIM, MSN Messenger, Google Talk, Yahoo Messenger, etc. This class of software is currently prohibited to be installed on any company owned computer, laptops and individually owned computers approved to connect to the company net due to potential security, bandwidth, and authentication issues.

5.01.19. Physical Security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. The following guidelines should be adhered to strictly by all personnel of the Company:

1. Diskettes and portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
2. Diskettes should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the IT manager is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.
6. Employees shall not take shared portable equipment such as laptop computers out of the plant without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that

may result.

5.01.20. Non-Corporate/Private Individual Owned Computer System

Individuals who desire to use a personal owned laptop computer system for Cycladic business purposes and have internal network access must have written authorization from the IT Manager; otherwise, individually owned computing equipment will not be connected to the Company's internal network in any fashion. Prior to receiving approval, the system must comply with and meet the hardware and software configurations required of company systems. This includes the installation and use of appropriate password, firewall, antivirus, and malware in accordance with the provisions of this policy manual.

5.01.21. Phones, Pagers, and Facsimiles

Employees are expected to limit the duration and frequency of personal phone calls (telephone and cellular), pages and facsimile transmissions and to conduct them in a professional manner. Excessive personal calls or pages during the workday can interfere with employee productivity or be distracting to others. It is the employees responsibility to ensure friends and family members are aware of the Company's policy.

Long distance access codes are assigned to authorized employees with the approval of their department manager. Employees are not to access company long-distance services using another employees access code, reveal their access code to unauthorized persons or purchase telephone billed services (e.g., using 900 numbers). Employees may be required to reimburse the Company for non-business telephone charges; provided, however, any director or executive officer of the Company must charge any non-business telephone calls to his or her own personal telephone number or credit card. The Company's toll free line is for business purposes only; employees are not permitted to use this line to receive personal incoming calls.

Employees whose job responsibilities include regular or occasional driving and who use a cellular phone to conduct business are expected to refrain from using their phone while driving due to safety concerns. The Company will not be liable for the loss of or damage to personal cellular phones brought into the workplace.

5.01.22. Acknowledgment of Information Security Policy

Compliance with the section BP 5.01 of Cycladic's Business Policy Manual is required. All employees must have a signed acknowledgment on file with the Human Resources Department (Appendix F).

BP 6.01 TRAVEL & ENTERTAINMENT POLICY

Cycladic Imports, Inc. has established this policy to provide employees with standard practices with regard to travel, entertainment and certain other reimbursable business expenses. The policy is designed to maximize the effectiveness of travelers, minimize costs to the Company, properly document expenditures in accordance with company policies, procedures and federal tax laws, and make timely reimbursement to the employee.

It is recognized that unusual situations will arise that may not be addressed by this policy. Additionally, the definition of “reasonable” may vary due to travel location, purpose of expenditure, etc. If an anticipated expenditure appears outside what may be considered “standard” or “reasonable,” advance approval by the employee’s supervisor is required. The overriding premise of this policy is that employee expenditures for reimbursement will be reasonable, have an appropriate, documented business purpose and be in accordance with the current *Business Conduct Policy* of Cycladic Imports, Inc.

6.01.1. Air Travel

Employees with business travel plans shall make required airline reservations as soon as possible to maximize the potential savings from purchasing tickets in advance. Coach Class shall be used for flights five hours or less in duration; Business Class may be selected for flights exceeding five hours. Any flight in excess of five hours may be upgraded to the next higher class if frequent flier coupons are utilized. Exceptions shall be appropriately approved.

Officers with business travel plans shall make required airline reservations as soon as possible to maximize the potential savings from purchasing tickets in advance. Coach Class shall be used for flights two hours or less in duration; First Class may be selected for flights exceeding two hours. Frequent flier coupons should always be utilized to upgrade to First Class if available. Exceptions shall be appropriately approved.

The employee or officer will make reservations with the approved travel agency on the airline offering the best fares available that meet the travel timetable provided by the employee. Receipts are required as support for reimbursement.

Unused/Exchanged Tickets – When flights are changed prior to departure, if new tickets are issued, the old tickets will be returned to the company’s authorized travel agency immediately to avoid additional charges to the employee’s credit card. Unused tickets (including non-refundable tickets) should be quickly returned to the company’s travel agency, which can get a credit for your unused tickets or use your non-refundable unused ticket and apply it toward another non-refundable ticket. Non-refundable tickets can be re-used (within a 1-year period) against other non-refundable tickets for an additional charge.

Lost Tickets – Lost tickets (issued by the company’s travel agency) will be reported immediately to the company’s travel agency. The company’s travel agency will complete and submit the

required paperwork to obtain refunds for lost tickets.

Frequent Flyer Credits – Travelers are free to acquire and use frequent flyer credits obtained from company paid trips. However, under no circumstances will a traveler purposely delay booking a trip, or insist upon a higher priced ticket when lower fares are available in order to gain frequent flyer credits.

Local Flights – Local flights, such as Southwest Airlines, should be booked directly with the airlines to avoid costly travel agency surcharges.

6.01.2. Ground Transportation

Rental Cars – All car rental reservations should be made through our approved travel agency even when no airline tickets are needed. Car rentals should be used when it is the most economical means of transportation. Travelers should use our preferred rental agency for the best rates. Cycladic Imports, Inc. employees can enroll as a Preferred Renter. These applications can be obtained through our approved travel agency.

Payment – Rental cars booked for company travel should be charged to the traveler's individual credit card. All personal rentals must be paid for by the employee.

Size – Travelers should use a full-size rental car, unless the number of people utilizing the car dictates a larger vehicle. If a larger car is required, list the names of the other passengers on the expense report.

Insurance (Domestic) – Employees shall decline additional insurance coverage (e.g., loss damage waiver or collision damage waiver) when renting automobiles for business purposes. The Company is self-insured for physical damage.

Accidents – If you are involved in an accident while driving a rental car, you must immediately notify your supervisor, the VP Finance office, the rental agency, and the local police. The employee has the responsibility to insure that a police report is made for all accidents involving the use of rental cars. If the employee is unable to get a police report, get witness' name, address, etc.

Parking & Tolls – All parking fees and tolls incurred while on company business will be reimbursed. Receipts should be attached to the employee's expense report. Any parking/traffic violations will not be reimbursed by the company. Each expense above \$20 requires a receipt.

Use of Personal Vehicle/Mileage Allowance – Mileage allowance for the use of your personal car for business purposes is at a designated rate allowed for by the IRS. Contact the Accounting Department for current mileage rates. In order to receive reimbursement, you must record the origin and destination of the trip, the business purpose and the miles claimed on your expense report/mileage form. You may claim mileage OR gas expenses but not both. Each expense above \$20 requires a receipt.

Taxi Service, Subway, Railroad & Bus Fares – The Company will reimburse employees for the reasonable cost of taxi, subway, railroad, bus fares, and limousines when appropriate. Each expense above \$20 requires a receipt.

Hotel/Lodging – Lodging, when traveling for the Company, will be approached economically. Employees should make it a practice to stay in intermediately priced rooms. The corporate rate or other best rate shall be requested when making reservations or at check-in. Employees are not expected to share rooms. Generally, employees shall pay for lodging at the time of checkout. Only in special circumstances shall employee lodging be billed directly to the Company. The reasonable cost of lodging will be reimbursed, if a receipt supports the expense.

Miscellaneous – Dry cleaning, personal entertainment, car washes on personal vehicles, and other incidentals are considered personal expenses and are not subject to reimbursement. Exceptions for dry cleaning or laundry may occur for extended trips (greater than three days) or in the event of an emergency. The cost of personal telephone calls home, which are reasonable in number and duration, will be reimbursed. The use of the mini bar is acceptable but good judgment is expected.

Meals – Meals are an allowable expense only when travel is involved in the conduct of Company business. Employees must submit receipts for all meal expenses incurred. Unless on travel status, the purchase of meals for other Company stakeholders is not a reimbursable expense except in those situations where the nature and sensitivity of the matters to be discussed are such that a breakfast, lunch or dinner meeting is clearly in the best interests of the Company.

In travel status situations where separate checks are inappropriate, the appropriate senior level officer or manager shall be responsible for payment of the meal expense and submission of the total expense on his/her expense report. Each person in attendance must be listed on the expense report.

6.01.3. Entertainment

Employees will be reimbursed for the reasonable cost of meals, beverages, and other entertainment expenses when there is a valid business purpose. A receipt is required for each expenditure over \$25. The following documentation is required:

- name, title and company of business guest(s) entertained;
- description of business relationship;
- nature or purpose for business discussion or activity; and
- name, location, and type of entertainment (if not evident from the name).

Cycladic Business Conduct Policy – The Company's *Business Conduct Policy* provides guidelines for employees to follow when entertaining business associates. Any question(s) about whether entertainment expenses are reasonable and/or appropriate shall be reviewed in advance with the employee's supervisor. It is the policy of the Company to reimburse employees for expenses incurred for business entertainment in accordance with the guidelines established below:

As a general rule, entertainment of business associates will be conducted by management. In the occasion where circumstances justify business entertainment by employees other than management, the prior approval of the employee's supervisor is required.

- Reasonable expense of entertaining and gifts for customers and prospects will be allowable provided such expenses are incurred for business purposes. The regular entertainment or meal record must be submitted for each occurrence, identifying the customer attending and the specific business discussed.
- The frequency of entertainment situations involving the same people should be controlled. Business relationships, ordinary and necessary to the promotion of the Company's affairs, must be the motivating factor. Discretion should be used in all entertainment activities and the number of Company stakeholders brought into the occasion should be kept to a minimum as dictated by good business practice and judgment.
- Entertainment expenses will be reimbursed only for business meals or in cases where the entertainment is directly related to, or associated with, the Company's business. It should be recognized that it is difficult to establish precise guidelines distinguishing business and personal entertainment, and management must therefore rely on the judgment and good faith of its employees in this area. Expenses for entertainment of a personal nature are not tax deductible by the Company and reimbursement will be denied in such cases.
- Requests for reimbursement of entertainment expenses must be approved by the employee's supervisor. Each expense receipt shall contain a detailed itemization of expenses incurred and a statement of the date, place and business reason for entertainment, as well as the names of those present and their business relationships to the Company. Expenditures of \$25.00 or more must be accompanied by receipts. No matter the cost, when receipts are available, they should be obtained.
- Entertainment expenses must be reasonable and will not be reimbursed to the extent that they are lavish or extravagant. An unusual or large expenditure for entertainment must be approved by management prior to the event.
- The Company will reimburse a supervisor or department for entertainment of his subordinate Company associates only when the department manager has approved the function in advance.
- All persons in attendance should be set out on the expense reporting form.

Gifts – Gifts, which shall be in accordance with the Company's Business Conduct Policy, are occasionally permissible, with the same business purpose requirement as entertainment expenditures. A receipt is required for each expenditure over \$25. The following documentation is required:

- amount, description, business reason for and date of the gift and
- name, title, company and business relationship of the gift recipient.

6.01.4. Cash Advances

Expense advances may be obtained by submitting an approved travel request form to the Business Expenses Department. Approvals are to be at the same level required for expense reports. An employee requesting an expenses advance shall submit a request form in advance of travel to allow sufficient time for processing. No expense advance will be made to any director or executive officer of Cycladic Imports, Inc.

Advances will be taken into account when the related expense report is filed. At that time, the employee will be reimbursed for expenses in excess of the advanced amount or the employee will reimburse the Company for the amount in excess of expenses.

6.01.5. Expense Reporting

Employees must submit expense reports for all business travel and entertainment expenses incurred on behalf of the company. Reports should be turned in on a timely basis. Requested reimbursements for expenses incurred greater than three months prior to the date of the report must be approved by the Vice President of Finance.

Any expenditures of \$25.00 or more must be supported by original vouchers or receipts (except for mileage reimbursements) specifying the quantity and kind of goods and services purchased. Reimbursement is based on this documentation and the absence of documentation must be explained. It is strongly advised that documentation for expenditures under \$25.00 should be submitted if available.

Where entertainment is involved, the name and address of entertainment establishment, names, and business relationships of those individuals or groups entertained, type of entertainment, and the business purpose must be stated on the expense account. Whenever unusual circumstances surround a particular expense, they should be explained on the form or an addendum thereto. Exceptions will be reviewed on an individual basis by the Vice President of Finance. Expense Reports should be submitted to the employee's supervisor for approval before being submitted to the Accounting Department. In the case of an officer, expense reports will be approved by another officer at the same level or higher than the officer submitting the expense report. All expense reports shall be approved at least one level higher than the employee. The expense reports of the Chief Executive Officer shall be approved by a Vice President of the Company. The employee and approving manager or officer are responsible for both the accuracy of the report and compliance with the requirements of company policies and procedures.

Completing The Expense Report – The Expense Report should be completed following the guidelines set out below:

- On overnight trips, the city in which the employee spends the night should be entered in the applicable space.
- Only daily room rate charges and room tax amounts should be listed on hotel/motel space.
- Meal charges including tips should be listed under the applicable meal space.
- Telephone, laundry, entertainment, etc. expenses should be listed on the appropriate line.
- The line for tips should include only tips for skycaps, bell hops etc. not for meals or entertainment.
- All rental car charges should be indicated on a separate line. The Auto Expense space should include personal auto charges including mileage and any gas charges incurred.
- Expenses charged on a credit card shall be listed as expenses on the expense report.
- When traveling internationally the employee shall indicate the purchase exchange rate of

each currency on the expense report and any supporting documentation necessary to support the exchange rate conversions.

- The U.S. dollar total shall be indicated on all receipts in foreign currencies.
- Receipts for currency exchange shall be attached to the expense report. These exchange rate differences are reimbursable by the company.

6.01.6. Cellular Telephones

Officers will be reimbursed for the monthly cost of one cellular telephone service. Rate plans are expected to not be excessive and meet the needs of the officer as appropriate. Billing statements will be included with the expense reports. Employees will be reimbursed for the actual costs of business calls on cellular telephones and the pro-rata portion of the base rate attributable to the business usage. Billing statements detailing the business use and pro-rata calculations will be included with the expense reports.

6.01.7. Internal Audit

Employee expense reports will be subject to review by Internal Audit. All expense reports for executive officers who are listed in the Proxy Statement for the annual meeting of shareholders of Cycladic Imports, Inc. will be reviewed within 30 days of submission. Exceptions to policy will be reported to the officer submitting the report and the approving officer for correction.

6.01.8. Miscellaneous

Unauthorized Expenses – It is not permissible for employees to request reimbursement for computer equipment and software through employee expense reports. Supplies, equipment, services, and other similar purchases generally shall follow standard purchasing practices for the employee's location.

Tips – Tips are covered expenses and in reasonable amounts will be reimbursed. A meal tip shall be included in the reported cost of the meal. The nature of tip expenditures that exceed \$25 per day shall be documented.

Spouse Travel – Travel expenses for spouses, which shall be approved in advance, will be reimbursed where it is necessary for the spouse to attend the function to achieve its business purpose.

Foreign Currency Translation – Expenses in foreign currency shall be translated into U.S. dollars by the traveler at a rate existing on the date the expenses were made. However, if a different rate is more appropriate to fully reimburse the traveler, it shall be used (such as the actual exchange rate used by the credit card company for charged expenses). Rates can be found in daily newspapers.

Membership Dues & Fees – Employees, whose majority use of a club meets the business purpose requirement, may be reimbursed for monthly membership dues upon approval of the Company

President and Chief Executive Officer. In addition, with this same approval, the Company may subsidize a club membership. Entertainment expenditures and documentation are subject to the same standards described elsewhere in this policy. Under no circumstance will personal expenses be reimbursed.

Annual membership fees for airline clubs and travel lounges will be reimbursed with prior approval of the appropriate individual. Annual fees for credit cards, up to \$100, may be reimbursed for employees who travel and/or entertain extensively.

Professional Dues & Fees – The Company, subject to prior approval of the appropriate Vice President, may reimburse the cost of obtaining and maintaining a professional license, certification, registration, or membership. It is expected that such memberships or associations would benefit the Company.

BP 7.01 SMOKING IN THE WORKPLACE POLICY

Cycladic Imports, Inc. takes pride in providing a clean and healthy workplace where our employees have the opportunity to develop their skills and talents. Because of medical studies linking higher illness rates to smoking and exposure to second-hand smoke and the expressed concerns of our employees, the Company has established this policy which prohibits smoking in the workplace.

Smoking is prohibited in all offices and common areas including, but not limited to, the following areas: offices, cubicles, training rooms, conference rooms, restrooms, hallways, eating areas, file space and reception areas.

BP 8.01 WORKPLACE ENVIRONMENT POLICY

8.01.1. Policy

Employees are responsible for assuring that the workplace is friendly and conducive to high productivity and exceptional performance. The Company expects all employees to avoid any action or conduct that creates a hostile or intimidating environment or constitutes sexual harassment or a threat or act of violence.

Sexual harassment may include unwelcome sexual advances, requests for sexual acts and/or favors or other physical or verbal conduct of a sexual nature, whether by supervisors, other employees, or non-employees. Sexual harassment exists when:

- Submission to sexual harassment is an explicit or implicit term or condition of employment, including hiring, compensation, promotion, and/or continued employment.
- Submission to or rejection of such conduct is a basis for employment decisions.
- Conduct has the effect of unreasonably interfering with an employee's work performance or creates an intimidating, hostile or offensive environment that interferes with work performance.

Examples of sexual harassment conduct include the following:

- *Verbal* – sexual innuendos, suggestive comments, jokes of a sexual nature, sexual propositions and/or threats.
- *Nonverbal* – display of sexually suggestive objects or pictures (including calendars and posters), suggestive or insulting sounds, leering, whistling and/or obscene gestures.
- *Physical* – unwanted physical contact, including touching, pinching, brushing the body, unwelcome sexual advances and/or assault.

Workplace hostility includes any verbal, physical or visual conduct that creates an intimidating, offensive or hostile working environment that interferes with work performance. Some examples include racial slurs, ethnic jokes, or posting of offensive cartoons.

8.01.2. Violence

Threats or acts of violence committed by or against any employee or non-employee on company property will not be tolerated. Threats or acts of violence include conduct against persons or property that is sufficiently severe, offensive or intimidating to alter the workplace environment or create a hostile, abusive or intimidating work environment for one or more employees. Violent activities include, but are not limited to, physical or verbal acts of harm to another individual, such as intimidating words or gestures, shoving, pushing, harassing, coercing, brandishing weapons, and threatening or talking of engaging in any of these activities.

8.01.3. Procedures for Reporting Harassment, Hostility or Violence

Employees shall report any observed act or conduct in the workplace that violates this policy to his or her supervisor or the General Counsel of Cycladic, Inc. (757-233-6170). In the event of violence or threatened violence, employees shall call "911." Any employee who believes that he or she has been the subject of any act or conduct in violation of this policy must immediately report the same to an appropriate company official to enable the Company to investigate and take appropriate action. No employee is required to report any violation directly to a person who is accused of violating this policy. All employees will be protected from coercion, intimidation, retaliation, interference or discrimination for filing a complaint or assisting in an investigation. Reports will be immediately investigated in a fair, impartial, timely and professional manner. Information included in the investigation will be kept as confidential as practical and will be discussed only on a need-to know basis.

These procedures are designed to encourage the reporting of workplace hostility, sexual harassment and threats or acts of violence and to provide appropriate confidentiality while enabling management to investigate. Any employee determined to have violated this policy will be subject to appropriate disciplinary action, up to and including termination. A non-employee, who subjects an employee to harassment, hostility, threats or acts of violence in the workplace, shall be informed of the Company's *Workplace Environment Policy* by the area supervisor or manager. Other action may be taken as appropriate, including possible banishment from company property.

BP 9.01 DRUG & ALCOHOL TESTING POLICY

9.01.1 Policy

It is the purpose of Cycladic Imports, Inc. to help provide a safe and drug-free work environment for our clients and our employees. With this goal in mind and because of the serious drug abuse problem in today's workplace, we are establishing the following policy for existing and future employees of Cycladic.

The Company explicitly prohibits:

- The use, possession, solicitation for, or sale of narcotics or other illegal drugs, alcohol, or prescription medication without a prescription on Company or customer premises or while performing an assignment.
- Being impaired or under the influence of legal or illegal drugs or alcohol away from the Company or customer premises, if such impairment or influence adversely affects the employee's work performance, the safety of the employee or of others, or puts at risk the Company's reputation.
- Possession, use, solicitation for, or sale of legal or illegal drugs or alcohol away from the Company or customer premises, if such activity or involvement adversely affects the employee's work performance, the safety of the employee or of others, or puts at risk the Company's reputation.
- The presence of any detectable amount of prohibited substances in the employee's system while at work, while on the premises of the company or its customers, or while on company business. "Prohibited substances" include illegal drugs, alcohol, or prescription drugs not taken in accordance with a prescription given to the employee.

The Company will conduct drug testing under any of the following circumstances:

- **RANDOM TESTING:** Employees may be selected at random for drug testing at any interval determined by the Company.
- **FOR CAUSE TESTING:** The Company may ask an employee to submit to a drug test at any time it feels that the employee may be under the influence of drugs or alcohol, including, but not limited to, the following circumstances: evidence of drugs or alcohol on or about the employee's person or in the employee's vicinity, unusual conduct on the employee's part that suggests impairment or influence of drugs or alcohol, negative performance patterns, or excessive and unexplained absenteeism or tardiness.
- **POST-ACCIDENT TESTING:** Any employee involved in an on-the-job accident or injury under circumstances that suggest possible use or influence of drugs or alcohol in the accident or injury event may be asked to submit to a drug and/or alcohol test. "Involved in an on-the-job accident or injury" means not only the one who was injured, but also any employee who potentially contributed to the accident or injury event in any way.

If an employee is tested for drugs or alcohol outside of the employment context and the results indicate a violation of this policy, the employee may be subject to appropriate disciplinary action,

up to and possibly including discharge from employment. In such a case, the employee will be given an opportunity to explain the circumstances prior to any final employment action becoming effective.

9.01.2. Rehabilitation

Employees who have a substance abuse or dependency problem are encouraged to seek medical attention for rehabilitation. Any employee who desires the opportunity to overcome substance abuse or dependency should contact the General Counsel for help prior to being reported for abnormal or unsafe behavior or being notified of selection for random testing. The Company's health plan provides medical assistance for precertified participants for the treatment of substance abuse and/or dependency. Rehabilitated employees will be required to complete the aftercare program prescribed by the treating medical provider and will be subject to appropriate surveillance upon returning to work.

9.01.3. Positive Results

The Company's drug and alcohol testing program is designed to safeguard employee and prospective employee rights. Positive drug test results (hair samples) will be confirmed and validated by a third party medical review officer ("MRO"). This process may require disclosure of information to the MRO about substances, drugs and medications taken during the period prior to testing. If an employee tests positive for illegal or unauthorized drug use, a retest may be requested at the employee's expense. If the employee does not request a retest, or the retest results are positive, the employee will be subject to termination. An employee with a positive test result for alcohol (breath test or blood or urine samples) will be subject to termination.

BP 10.01 PERSONNEL RECORDS POLICY

Cycladic Imports, Inc. recognizes its responsibility to maintain the confidentiality of its employee records and has established safeguards for the protection of personnel records on present and past employees. Access to personnel files is limited to a need-to-know basis for administrative and supervisory purposes only.

Employees are responsible for notifying the Vice President and Chief Financial Officer of the Company whenever there is a change of address, telephone number, marital status, dependent status, persons to notify in case of emergency, and changes in educational status. Active employees may review their personnel records by appointment and in the presence of the Vice President and Chief Financial Officer. No records may be removed, reproduced or altered. All written or telephone inquiries relative to current or previous employees shall be referred to the General Counsel (757-233-6170) in an effort to control the disclosure of information. No employee other than the General Counsel may respond to requests for references or information about current or previous employees. Requests for such information shall be answered by stating that the Company has a policy requiring that this information be furnished only by the General Counsel.

The General Counsel will respond to requests for dates of employment and job titles only. Information relative to reasons for termination and job performance will be furnished only after receipt of an authorized release executed by the employee, or former employee, except as required by law.

Appendix A – Cycladic Approved Software List

Note: This is the approved software list – inclusion on this list does not mean that the software is currently available or licensed for use withing Cycladic Imports, Inc.

Operating Systems

- MS Windows 2000 Server
- MS Windows 2000 Professional
- MS Windows XP Professional
- MS Windows 2003 Server Standard
- MS Windows 2003 Server Enterprise
- Red Hat Linux 9
- Fedora Core 4
- FreeBSD 5.4

Core Applications

- Diskeeper 10 Pro
- MS Office 2003
- MS Windows SQL Server
- MS Windows ISA Server
- MS Windows Exchange Server
- MySQL
- SAP Business Suite
 - Customer Relationship Management
 - ERP
 - Product Lifecycle Management
 - Supply Management
 - SAP Analytics
 - SAP Manufacturing
 - SAP Service and Asset Management
 - SAP xApps
- McAfee VirusScan Enterprise 8.0i

Departmental Applications (Use is restricted to specific departments)

- Adobe Page Maker
- MS Visio
- Macromedia
 - Dreamweaver MX
 - Fireworks
 - Freehand
- OmniPage Pro
- TextBridge Pro

Appendix B – Blocked Mail Attachment Types

1. ade - Microsoft Access project extension can contain executable code.
2. adp - Microsoft Access project can contain executable code.
3. app - Microsoft FoxPro application is executable code.
4. asp - Active server pages
5. asx -
6. bas - Basic program source code is executable code.
7. bat - Batch file which can call executable code.
8. chm - Compiled HTML help file can contain executable code.
9. cmd - Windows NT command script file is executable code.
10. com - Command file program is executable code.
11. cpl - Control panel extension
12. crt
13. csh
14. dll - Dynamic link library is executable code. Could be placed on your system then run by the system later.
15. exe - Binary executable program is executable code.
16. fpx - Microsoft FoxPro is executable code.
17. hlp - Help file
18. hta - HTML program
19. inf - Setup information
20. ins - Internet naming service
21. isp - Internet communication settings
22. js - JavaScript file
23. jse - JavaScript encoded file
24. ksh - Unix shell file
25. lnk - Link file
26. mda - Microsoft Access add-in program
27. mdb - Microsoft Access program
28. mde - Microsoft Access MDE database
29. mdt - Microsoft Access file
30. mdw - Microsoft Access file
31. mdz - Microsoft Access wizard program
32. msc - Microsoft Common Console document
33. msi - Microsoft windows installer package
34. msp - Windows Installer patch
35. mst - Visual Test source files
36. ops - FoxPro file
37. pcd - "Photo CD image or Microsoft Visual Test compiled script"
38. pif - "Shortcut to MS-DOS program"
39. prf - "Microsoft Outlook Profile Settings"
40. prg - "FoxPro program source file"
41. reg - Registry files

42. scf - "Windows Explorer Command file"
43. scr - Screen saver
44. sct - Windows® script component
45. shb - Document shortcut
46. shs - Shell scrap object
47. url - Internet address
48. vb - Visual Basic file
49. vbe - Visual Basic encoded script file
50. vbs - Visual Basic file
51. vsd
52. vss
53. vst
54. vsw
55. wsc - Windows script component
56. wsf - Windows script file
57. wsh - Windows script host settings file
58. xsl - XML file may contain executable code
59. zip - Many viruses are commonly zipping files to keep them from being scanned and providing instructions to users about how to run the attachment. Many users still do this so to secure the network, it has become necessary to block this attachment type.

Appendix C – Visitor's Log Form

Cycladic Imports, Inc.
Visitor's Log

Date	ID #	Time In	Time Out	Name	Company	Visiting/Purpose

Appendix D – Key Escrow Form (KE-1)

Purpose

This form is to be used whenever Cycladic employees protect sensitive company information using encryption. These forms will be stored in a physically protected location by the Office of Compliance, and will be used in the event that data recovery is required.

Required Information

Employee Name _____ Date _____

Employee Title _____

Description of Data Being Protected _____

Location of Data Being Protected:

System or Server Name _____

Full Filename (including directory path) _____

Software Providing Encryption _____

Key or Passphrase _____

Appendix E - Disaster Recovery & Emergency Check List

- I. CONTINGENCY PLAN FOR MAJOR DISASTERS
 - A. Detection and Reaction
 - i. Identifying the problem; Notifying the authorities
 - a) Emergency services
 - b) Environment
 - c) Physical security
 - ii. Reducing Cycladic's exposure
 - a) Air-conditioner failure
 - b) Fire alarm procedure
 - c) Electrical-failure procedures .
 - d) Flood and water damage
 - iii. Evacuation of the facility
 - iv. Advising the Emergency Management Team of the situation
 - v. Creating a flow chart of the detection and response
 - B. Initiation of Backup-Site Procedures
 - i. Emergency Management Team notifies other teams
 - ii. Establish Control Center
 - iii. Begin Disaster Recovery Team operations and Disaster Recovery Logs
 - iv. Timed events
 - a) 1 to 6 hours after being notified
 - b) 6 to 12 hours after being notified
 - c) 12 to 24 hours after being notified
 - d) 24 hours after being notified
 - C. Establishment of Full Recovery at Backup Site
 - i. All planned software, hardware, and resources in place at backup site, and the applications tested
 - ii. Communications network and other equipment fully operational
 - iii. Disaster Recovery Team checklists
 - D. Restoration of Facilities and Operations at the Original and/or Alternate Site
- II. DISASTER RECOVERY TEAMS
 - A. Departmental Organizational Chart
 - B. Description and Responsibilities
 - i. Disaster Planning Coordinator
 - ii. Emergency Management Team
 - iii. Operations Team
 - a) Computer operations
 - b) Facility preparation
 - c) Replacement hardware
 - d) Cold-site preparation
 - e) Computer support equipment
 - f) Supplies

- iv. Data Entry and Control Team
 - a) Data input
 - b) Data control
- v. Special Projects Team
 - a) Transportation to/from backup facilities
 - b) Training
 - c) Administrative services
- vi. Technical Support Team
 - a) System software
 - b) Communications network
- vii. Data Administration Team: Database Restoration and Integrity
- viii. Systems and Programming Team
 - a) Application systems restoration and recovery
 - b) Application programs
- ix. Insurance Department Team: Insurance and Salvage
- x. Internal Audit Department Team: Verification of the Integrity of Restoration Operations
- C. Team Pre-planning and On-Going Functional Responsibility
 - i. Disaster Planning Coordinator
 - ii. Emergency Management Team
 - iii. Operations Team
 - iv. Data Entry and Control Team
 - v. Special Projects Team
 - vi. Technical Support Team
 - vii. Database Team
 - viii. Systems and Programming Team
 - ix. Insurance Department Team
 - x. Internal Audit Department Team
- III. DATA CENTER REQUIREMENTS
 - A. Computer Room and Tape Library Layout
 - B. Power Requirements, Cable Diagrams, and Plug Connectors
 - C. Air-Conditioning, Fire Protection, and Security
 - D. Computer Equipment and Vendor by Location and Serial Number
 - i. Computer room
 - ii. Data entry
 - iii. Other areas: Programming/systems/technical services/offices
 - E. Teleprocessing: Configuration Information
 - i. Line flow chart drawing
 - ii. Communication controller (3705)
 - iii. Satellite 64
 - F. Terminal Configuration Charts
 - i. Local terminal configuration
 - ii. Remote terminal configuration

Appendix F – Employee Acknowledgment Form

Acknowledgment of Information Security Policy

This form is used to acknowledge receipt of, and compliance with, Cycladic Imports, Inc. Information Security Policy.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the information services manager.

Signature

By signing below, I agree to the following terms:

- i. I have received and read a copy of the “Information Security Policy” and understand the same;
- ii. I understand and agree that any computers, software, and storage media provided to me by the company contains proprietary and confidential information about Cycladic and its customers or its vendors, and that this is and remains the property of the company at all times;
- iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at Cycladic, otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
- iv. I agree that, if I leave Cycladic for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.

Employee signature: _____

Employee name: _____

Date: _____

Department: _____

Disclaimer

This Business Policy Manual is meant for educational purposes only. It does not purport to be complete or error free with the respect to the information contained herein. Any resemblance to real persons living or dead or any corporation is purely coincidental.

Acknowledgment and Copyright

This document was originally prepared by Del Mar College for the 2006 Southwest Collegiate Cyber Defense Contest (SW-CCDC), and was subsequently modified for the 2007 SW-CCDC by Steve Tate at the University of North Texas. All rights reserved – if you wish to use parts of this document, please contact Steve Tate at srt@cs.unt.edu for information and permission.