APPENDIX 1

Appendix 1: Seriousness/Impact Assessment Guidelines

Consequences of Disclosure, Modification or Loss

Company Operations	LEVEL 1 Moderate Damage (Low) 50%	LEVEL 2 Significant Damage (Med) 45%	LEVEL 3 Irreparable Damage (High) 5%
Intellectual capital (patented or proprietary material)	Legal defence of IPR required	Protracted legal defence of IPR required	Permanent loss of material
Statutory or Regulatory controls (FDA, EMEA etc)	Issue of regulatory body document of censure (e.g. FDA 483)	Regulator warning/suspension of R&D function, or project	Permanent closure of R&D function or project (prosecution or litigation)
Delay to operations/product pipeline (impact on revenue flow)	Impact on operations, but no delay to product pipeline and projected revenue flow	Impact on operations and/or delay to product pipeline of up to one month	Unable to operate and/or product pipeline delayed by over one month
Harm to Health, Safety and the Environment	No immediate harm to EHS, but a source of concern requiring investment internally	Harm caused to EHS, manageable but a cause of concern to external community. Manageable Regulatory intervention	Harm to EHS which is difficult to manage and/or a major cause of concern externally. Regulatory intervention and/or litigation w/major impact.
Breach of core values/good management procedures	Undermining of confidence in Divisional Management/breach in core values	Undermining of confidence in Company Management/breach in core values. Possible civil litigation or Data Protection Commissioner (UK) intervention	Protracted civil or criminal litigation; intervention resulting in published ruling and punitive measures against Company
Media and Focus Group criticism	Local media and/or focus group criticism requiring remediation	National or international media and/or focus group criticism permitting a manageable media response w/limited impact	National and International media and/or focus group criticism causing major revenue or share impact
Financial Impact	Contained within normal parameters of business risk management	Significant financial loss or penalties, but share price impact containable	Tangible medium-term or longer impact on revenue, expenses or share price
Sensitive commercial information release	Short-term loss of revenue due to external agent (i.e. hijacking of materials, major protests at site)	Result in threat to employees or assets requiring Company response and significant expense	Permanent damage or injury to Company employees, assets or the public due to criminal or unethical activity

Disclosure of Management Information	Within acceptable business parameters	Outside acceptable parameters, but manageable within the Company/Corporation	Manageable only with outside assistance e.g., litigation or government intervention

The word "threat" is defined as, "an indication of impending danger or harm". Where trade secrets and proprietary information is concerned, threats come from a variety of places, including:

- Insiders — Contractors, Employees, Ex-Employees, Partners
- Hackers — Active and Passive
- Competitors — Gain access to trade secrets
- Press — May publish controversial stories
- Activist groups — Disagree with practices
- Foreign Governments — Information Warfare

When considering threats, analyze the likelihood that the threat possesses the **opportunity, motive, intent and skill** to warrant controls implementation. ***Vulnerabilities*** are those aspects of process design and/or implementation that increase a threat's likelihood by increasing opportunity, providing motive, attracting interest, or decreasing the skill or resources required to mount an attack. High threat levels combined with high vulnerability levels greatly increase risk.

A high threat level should be met with equally high degrees of control to reduce vulnerabilities, and more frequent review of available intelligence. Threats are often viewed as local; however, XYZ Inc.Net and use of the Internet broaden the areas of potential information threats to a global level. The following table provides a means to articulate the perceived threats to an information asset/object:

Likelihood Threat/ to Disclosure, Modification or Loss	
Threat Level	**Define all internal and external threats for the information or processes under review and assess them as follows:**
3 HIGH	Specific Intelligence, recent events, or the Company's or its employees' particular circumstances indicate they are a high priority target and/or a threat is imminent. If the information in question could have a high financial or scientific value to competitors if stolen, could be used to embarrass XYZ Inc., or could be used to harm XYZ Inc.'s operations, then it is more likely to be chosen as a target. If the information is easy to understand (information rather than data), and is relatively easy to find (e.g., a correlated database as opposed to separate systems) then it is more likely to be an object of illicit activity.
2 Significant	Recent general intelligence, the overall security climate and the Company's or its employees' individual circumstances indicate they are likely to be a priority target and/or a threat is possible

1 Moderate	The Company's or its employees' circumstances indicate that there is a potential for them to be targeted by extremists, competitors and/or the media
0 Low	There is nothing to indicate that extremists, competitors and/or the media would target the Company or its employees.

APPENDIX 2

Appendix:2: Guidelines for identifying, retrieving and preserving Computerized Evidence

Background:

Computers by their very complex and dynamic nature are prone to many kinds of adverse incidents. Adverse incidents can occur intentionally and unintentionally. These guidelines are intended primarily for intentionally caused incidents of sabotage, intrusion, misuse or other information security related incidents involving XYZ Inc. computers. Adverse incidents caused by things such as faulty software or hardware, power fluctuations and natural disasters should be dealt with in accordance with existing disaster recovery plans.

Computer incidents caused by malicious acts, abuse and misuse often require additional steps beyond those set forth in disaster recovery plans. In the event that the evidence guidelines conflict with disaster recovery guidelines, the business unit manager and information security officer should jointly resolve the conflict. It is recognized that strict compliance with best evidence practices may not be possible in all instances, especially when there are urgent business needs to get a computer or network back online. When decisions of this type are made, they should be documented so that a reasonable response can be given to potential legal questions that may arise at a later date.

Identifying intentionally caused adverse computer incidents:

Intentionally caused incidents can be initiated from inside or outside of the XYZ Inc. network. Internally initiated incidents almost always involve violations of corporate policies. They may be best identified by way of examples. They may include, but are not limited to:

- Maintaining offensive material on the XYZ Inc. network or on any XYZ Inc. owned computer.
- Using the XYZ Inc. network to download offensive material from the Internet or to transmit offensive material anywhere.
- Email harassment.
- Transmitting proprietary information to unauthorized recipients.
- Unauthorized scans of the firewall.
- Sabotaging any XYZ Inc. software of computer equipment.
- Facilitating the theft of trade secrets.

Examples of intentionally caused incidents initiated from outside the XYZ Inc. network can include:

- Unauthorized scans of the XYZ Inc. firewall.
- Unauthorized access to the XYZ Inc. network or to any XYZ Inc. computer.
- Introduction of a computer virus, worm or
- A denial of service attack against the XYZ Inc. network or any network application, files or segment.

Many of these incidents may also be violations of the law (both criminal and civil). Since it is usually not possible to determine in the early stages of an incident whether or not it will result in litigation, it is best to treat all incidents as if they would ultimately end up in court. This means that whenever possible, evidence should be preserved in its original form, and it should be handled and maintained in a manner that will prevent it from being altered.

Identifying Computer Evidence:

Once it's been determined that an intentional incident has occurred, evidence must be recovered and preserved. Integrity of the evidence must also be maintained while it is being stored. Otherwise, any effort spent recovering and preserving the evidence can be wasted if an incident results in litigation. Depending upon the nature of an incident, both hardware and software can be considered as evidence.

The key to determining what is evidence, and what is not, is to think in terms of what it will take to understand and demonstrate what occurred and how it occurred. If hardware is damaged as a result of an incident, then clearly, the original damaged hardware is evidence. If a particular piece of hardware played an integral role in an incident, and if the incident could not have occurred on a different piece of hardware, then that device could be considered as evidence. In many instances, it may be preferable to preserve a component in a piece of hardware such as a hard drive instead of the entire computer in which the drive was installed.

Retrieving Computer Evidence:

Failure to retrieve all evidence could limit or make it impossible to investigate what occurred. In all instances "original" evidence is the best evidence. If disaster recovery plans have been implemented, a decision must be made as to whether or not it is feasible to retrieve the evidence, and if so, which evidence to retrieve. As stated earlier, the Information Security Officer and business unit manager should be jointly involved in this decision. In an ideal world, "all" evidence should be retrieved and productivity would not be effected. In the real world, particularly in a network environment, it is not unusual for there to be a trade off between recovering evidence and resuming operations.

If the incident occurred entirely on a stand-alone computer or workstation, retrieval can be as simple as removing and preserving the hard drive for later imaging. The best practice in that instance is to remove the original drive, and replace it with a spare drive on which a backup can be restored. If that is not possible, a mirror image of the entire drive (including unallocated space) should be made. A DOS bootable floppy disk should be used so that original evidence, particularly date and time stamps, are not altered during the copy process. The original hard drive should not be booted under any circumstances prior to making the image copy, and preferably not at all. If no other alternative is available, the entire file system on the original drive, including hidden and system files should be copied. This practice, however, is not encouraged because date and time stamps can be altered and information in unallocated space cannot be examined.

Whenever possible, "hot Swappable" hard drives should be available to facilitate retrieval of evidence and restoring online services. If the computer is attached to the network and the incident also occurred on the XYZ Inc. network, it might also be necessary to retrieve network directories, log files and email on the email server. Basically, any and all directories and log files should be retrieved that would be necessary for the reconstruction of events.

Transporting Computer Evidence:
Computer evidence should be hand carried to Corporate Security whenever possible, but when that is not practical, it should be shipped via overnight delivery service. The package containing the evidence should be sealed with the sender's signature across a seam so that it would be noticeable if opened.

Chain of Custody:
A chain of custody record should be maintained with the evidence. It should contain a description of the evidence and the signature, and date and time received by each person handling the evidence. Note: description of evidence does not need to be in great detail, but should be specific enough to make it distinguishable from other similar evidence submitted in the same incident. For example, if two hard drives were being submitted as evidence, they should be described separately to include make, model and serial number of each drive and make model and serial number of the computer from which each drive was removed. It would not be sufficient to simple say "enclosed are two hard drives". If the evidence does not have a serial number then the description should contain enough information to clearly distinguish it from other evidence being submitted. If necessary, mark the evidence with an indelible marker.

Preserving Computer Evidence:
Each item of evidence should be marked with the initials of the person submitting it and the date it was preserved. Computer evidence should be secured in a safe, or in a locked room until it can be turned over to or shipped to Corporate Security. Access to the locked room should be limited to as few people as possible. A list identifying all people having access to the evidence should be sent to Corporate Security along with the evidence.

Privacy Laws and Local Jurisdictions:
It is recognized that privacy and data protection laws may differ from one country to another. These guidelines are intended to be a set of general procedures to follow in the event of intentionally caused adverse incidents on XYZ Inc. owned computers, and shall not override existing local laws. If any questions arise with regard to conflicts between any procedures described herein and local laws, they should always be resolved in compliance with existing laws. Consult with your local XYZ Inc. attorney for a legal opinion.