INFORMATION SECURITY POLICY FOR USERS

Introduction

This information security policy is the first step on the route towards the (improved) management of information security within our own organisation. Alongside physical security and securing the IT systems, we also hope to increase employees' security awareness.
This document forms part of the Jumbo Fish Farm Information Security Manual.

1. Definitions

- Information security: Implementing and maintaining a cohesive package of measures for securing the availability, integrity, confidentiality and exclusivity of the information provision.
- Company: Jumbo Fish Farm and all its operating companies, outlets or branches. Operating company: Operating company owned and/or managed by Jumbo Fish Farm.
- User(s): Employees, consultants, temporary workers and others working for and at the company, including personnel associated with third parties making use of the company's IT systems.
- IT systems: General description for computers, network, software, services such as Internet access or e-mail, ERP systems etc.
- Manager: The (line/departmental) manager, team leader or contact person (for external users) to whom the user is responsible.
- IT department: The organizational unit responsible for managing the company's ITsystems.

2. Objective

The objective of the information security policy is to maintain adequate information security to protect the Jumbo Fish Farm systems and prevent loss or damage and improper use of the same. This policy defines the rules which must be observed to bring about this security and to guarantee the safe and reliable operation of the Jumbo Fish Farm systems.

3. Scope

This policy applies to all users within the company, including all personnel associated with third parties. The policy applies to all information sources owned or leased by the company.

This document applies to the company holding and all its operating companies, outlets and branches. Given that some operating companies already have an internal information security policy, this document assumes the function of a main document.

Should there be any conflict between the company policy and local regulations, national legislation will prevail.

4. Deployment and management approval

The company's Board of Directors attaches great importance to information security and supports all policy measures approved by the company's Information Security Committee wherever applicable.

5. Roles and responsibilities

Responsibilities in the field of information security are assigned as follows:

- Managing Director: responsible for the security of information and systems within the entire company.
- Operations Manager/Controller: responsible for implementing the information security policy.
- Department Managers: responsible for the use of policy and guidelines in the field of information security,and checking it within the respective departments.
- Departmental heads: checking and reporting bottlenecks in the information security policy.
- Information Manager: support during policy implementation and responsible for developing the guidelines for improving information security, and responsible for the implementation of guidelines for applications.
- HR Manager: support during the implementation of the policy and

responsible for developing HR instruments to promote policy implementation.

6. Information security

Employee-related security

Employees must be aware of the threats to, and the importance of, information security, and must have access to the right resources, knowledge and expertise to this end. If either necessary or desirable, the company should provide (supplementary) training to enable employees to work appropriately with the systems.

The personnel policy contributes to this, for example by including security aspects in job descriptions, through confidentiality declarations, through including the employee's responsibility in the field of information security in the employment contract, or through detailing codes of conduct.

Every employee has a duty to report security risks and incidents and must never abuse or misuse the Company's ICT systems or improperly divulge personal information as defined by Kenyan law.

Employees' attention is drawn to their responsibility for utilising effective access security, particularly with regard to the use of passwords and securing user equipment.

Employees' attention is drawn to the security risks inherent in electronic office systems (e.g. computers, laptops, mobile phones, e-mail etc.); these systems entail a risk to the confidentiality of company data.

The use of IT company resources for private purposes, such as access to the Internet and sending personal e-mails, should be kept to an absolute minimum.

Clean Desk policy

A clean desk policy protects documents against undesirable attention for security purposes and to ensure the confidentiality, integrity and availability of documents.

For this reason, take note of the following:

- During the absence of an employee, papers and digital documents must be stored away in such a way that they are not accessible to third parties but are available to colleagues who may need them. This applies not only to paper documents but also to confidential information on other information carriers such as USB flash drives, floppies, CDs, DVDs etc.

- During absences, the computer's screen protection should be engaged.
- The trays, baskets etc. for In, Out and Pending should only be used for the intended purposes.
- Items which are not intended for an employee should be returned immediately to the right person.
- Items which are not specifically required or which could be found elsewhere should be stored away immediately or destroyed.
- Attempts must be made to deal with matters as soon as practicable.
- Completed matters should be stored at least once a day in a (personal) archive.
- Paper in an open wastepaper basket or rubbish bin can also fall into the wrong hands. Confidential items should always be consigned to a closed wastepaper bin or to the shredder and destroyed immediately. This does not apply to information or documents that the law requires to be kept for a minimum period of time.

Electronic systems

In terms of the confidentiality of company information, employees are required to treat the use and sending of e-mails and access to the Internet with the greatest care.

The following statements articulate the company policy on security:

1. All information present on IT systems must be subject to limited access via usernames and passwords. Passwords must contain at least six characters. A complex (strong) password should be used, comprising capital letters, figures and if possible other symbols. Passwords must be changed at least once every six months. The IT department is responsible for reporting this in good time. Users are responsible for their own password and for what happens under their own login name.
2. Screensavers must be activated on all computers after 15 minutes. The screensavers must be protected with a password. The IT department is responsible for ensuring the adequate implementation of this.
3. An attempt to get around the security or to change data without permission is an offence, regarded as a serious contravention of the worker's employment

agreement which will ultimately lead to disciplinary measures, including possible dismissal.

4. If a user notes that he or she has too many rights allocated for certain IT systems, it is his or her responsibility to report this to the IT department. Should anyone misuse computer systems or suspect access by unauthorised users, he or she must notify the manager of this.
5. All users with access to information-sensitive applications must be suitably trained, including in the requirements for data security.
6. If an employee’s work contract is terminated, that user’s access to the company’s IT systems must immediately be blocked.
7. Anti-virus software is installed on all computers by the IT department. If viruses are reported, the IT department must be notified immediately, and the file or drive in question may no longer be used.

7. Computer software

Unlicensed duplication or unlicensed use of any type of software is illegal and could lead to the user and the company being prosecuted pursuant to the Copyright Act. Making unauthorised copies of software will not be tolerated by the company.

The following statements articulate the company policy on using computer software:

1. In terms of computer software, the user will only use such software in accordance with the licence agreement.
2. The user will not download or upload software via the Internet unless authorized by management for cases where such software is related to the Company’s business and promotion of its objects.
3. Users who note that software or related documentation is being misused within the company, must notify the manager or the IT department.
4. Company computers are checked periodically to see what software is installed. This configuration is compared against the official software list. Should unauthorised software be encountered, the person responsible for the computer will be contacted and may be subject to disciplinary measures.
5. Should there be any doubts as to whether a user may copy or use a specific software program, the IT department must be contacted before proceeding.

6. Infringement of the requirements above will be regarded as a serious contravention of a worker's employment agreement which will ultimately lead to disciplinary measures, including possible dismissal.

8. E-mail communication and Internet use

The company's e-mail system is the only e-mail program which may be used for sending and receiving e-mails.
E-mail as set up by the company is intended for use as a company resource. To this end, e-mail is subject to the company's normal security measures, specifically with regard to the absence of privacy in relation to the business of the company, despite the fact that there may be circumstances where it is permitted to use the e-mail system for personal use.

The company needs to ensure that neither the company nor users may be liable to external legal measures arising from the content of e-mails. The stipulations laid down in this policy document are intended to give substance to this objective. To avoid claims being lodged, all users must abide by these stipulations.

It should specifically be noted that e-mail is subject to the normal rules on libel or defamation. Employees are required to exercise significant care, either regarding oral or written information, or in the choice of recipient/s, both within the company and externally, where this might lead to legal measures against the user and/or the company. To this end, insulting language must be avoided, and the company will not in any way tolerate discrimination/intimidation on the grounds of race, gender, handicap, religion, age or sexual orientation; anyone conducting themselves in such a way will in all probability face disciplinary measures, including possible dismissal.

The e-mail address allocated to the user is the company's property and must be regarded as such. Accordingly, there is no right to privacy, and the user must assume that all e-mails and any attachments he or she sends and/or receives within the company or externally may be studied and/or recorded. An employee's use of the Internet (such as details of the sites visited) may also be tracked and/or recorded. It is particularly relevant to note this in terms of these rules if e-mail or the Internet are used for non work-related purposes.

The following types of files may not be sent and/or downloaded from the Internet: games, offensive images, pornography, political material, chain letters, junk mail, screensavers, applications and audio/video files.

Viruses

The company system is a closed one to the extent that it is not permitted to link peripheral equipment to the network without prior permission from the IT department.

E-mail attachments are filtered and files whose format constitutes a high risk are deleted. The filtering procedure applies to all mail exchanges between the company network and external mail systems (Internet). It is possible that attachments to personal e-mails which are regarded as offensive or posing a danger to the network will not be forwarded to the recipient.

Virus warnings of any type and from any source may only be forwarded for assessment to the IT department. The IT department is responsible for distributing relevant virus warnings; virus warnings emanating from any other source must be ignored. The reason for this that a large number of fake e mail warnings (hoaxes) are distributed, expressly intended to overload e-mail systems.

Internet use

The following statements articulate the company policy on using the Internet:

1. Access to the Internet is at one's own risk. The company is not responsible for material which is either viewed on or downloaded from the Internet.
2. Access to the Internet is a resource to assist the employee in his or her duties. Limited incidental personal use is, however, tolerated as long as it occurs in the user's own time and does not constitute an infringement of the stipulations in this company policy.
3. The user may not download any software from the Internet without specific permission from the Manager and the IT department.
4. The user may not distribute any information via the Internet which is critical of the company or confidential.
5. User access to the Internet may only occur via the method approved by the company. The user is not permitted to install his or her own Internet access on a

company computer. The use of non standard browsers can be approved and installed on dedicated (testing) equipment by the IT department.

6. An employee is not expected to act in such a way as to waste computer resources or time. Such acts include excessive surfing on the Internet, viewing non-business related streaming content, playing games, participating in chat groups on the Internet and using non-standard instant messaging-applications. The Jumbo Fish Farm Standard for instant-messaging integrates with other
7. instant messaging platforms.
8. Users have access to computers and Internet access in support of their duties. The user may not expect that the personal nature of material associated with the use of company computers will be respected.
9. The company records Internet activity routed via Jumbo Fish Farm Internet gateways using the relevant software.
10. The company deploys software to identify and block inappropriate material. The user may request and be granted access to Internet-sites that are normally blocked if there are no IT-risks and a clear business reason has been demonstrated.

9. Use of laptops and working from home

Some users have access to laptops. Securing and administering these computers is vitally important.

The following statements articulate the company policy on using laptops (applicable to users for whom a laptop has been made available):

1. As far as possible, the user must store data on the company server. If the hard drive is in fact used, the user is responsible for making backups and for storing these in a safe location. The IT department is responsible for installing the relevant software.
2. No software may be installed on the computer without prior discussion on the matter with the IT department. See the chapter on computer software.
3. Software for personal use may not be installed on the laptop, even if the user is in possession of a valid licence.
4. The user must take reasonable precautions to ensure the security of the computer. Do not leave it unattended (certainly not in a car), keep an eye on the

computer when travelling, and do not allow it to be used by unauthorised individuals.

5. Security measures must be taken to prevent unauthorised access to sensitive and confidential data. A start-up password must be in use at all times.
6. The company has a solution for remote access to the company's IT systems. Acceptable user policy applies to the use of this remote access ability. An employee may be held responsible for any misuse.
7. As a laptop user, the employee must log in to the company network regularly to ensure that the latest security updates are installed on his or her computer.

10. Management of information security

The Information Security Committee is primarily responsible for checking, assessing and maintaining documentation relating to company information security. The Information Security Committee reports at fixed times to the company CFO.

11. Consequences of regulation infringements

Non-compliance with the stipulations of the Information Security Policy for users and any misuse of the company IT systems which arises from this, or any other infringement of the security policy, will be regarded as a serious contravention of a worker's employment contract and will generally lead to disciplinary measures, including possible dismissal.

12. References

For further information about the company's security measures within the context of information security, norms, guidelines and measures, employees are referred to the *Jumbo Fish Farm Information Security Manual* or such other or further guidelines, directives or orders as may be given, issued or made by Management.