UGU – SOUTH COAST TOURISM (PTY) LTD

IT and COMMUNICATION POLICY

APPROVED 24 JANUARY 2012
Section 10: IT Disaster Recovery included & approved: 25 April 2013
Reviewed: 13.11.2013 : Tabled for BOARD APPROVAL : 5.12.2013

Contents

1. DEFINITIONS

In this policy, unless the context otherwise indicates, a word or expression to which a meaning has been assigned in the Act has the same meaning as in the Act, and-

a) **"entity"** means Ugu – South Coast Tourism

b) **"community"** means that body of persons comprising:

- **residents** of the municipality
- **ratepayers,**
- **any civic organisation and non-governmental, private** or labour organisation involved in the local affairs,
- **visitors** and other people residing outside the municipality, who make use of the services or facilities provided by the municipality, and
- includes more specifically, the poor and other **disadvantaged sections** of such body or persons

c) **"communication"** means the effective ways in which information is disseminated from sender to receiver and vice versa

d) **"area committee"** means representatives from each area elected to facilitate community participation in matters of the entity

e) **"key communicator"** means a person who is responsible for the effectiveness of communication

f) **"communication vehicles"** means a tool used to communicate

g) **"ratepayer"** in relation to a municipality means a person who is liable to the municipality for the payment of:

- rates on property in a municipality
- any other tax, duty or levy imposed by the municipality

h) "**regularly"** This refers to the changing of a password. The option is clearly managed for each user and is set to a standard number of days (40) between forced changes.

i) **"security breach**" Attempting to:

(i) attain access to network hardware/software, which is not officially assigned/installed for the official.

(ii) run/execute programs which were not set-up by the municipality.
(iii) change default hardware/software settings without prior consultation with and approval from the municipality.
(iv) login to the network using unauthorised user ID/s that were not assigned to the official.

j) **"applicable responsible person"** to report security breach of security to the "applicable responsible person" refers to for example an immediate supervisor or system administrator who will take further relevant action/steps.

k) **"any other media**" E.g. Stiffy or CD/DVD, mass media storage device/s or any other medium on which data can be stored or read electronically.

l) **"eliciting**" Dispose; elicit information.

m) **"cryptography"** The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text.

n) **"encryption"** Any procedure used in cryptography to convert plain text into cipher text (i.e. text which has been encrypted by some encryption system) in order to prevent any, but the intended recipient from reading the data.

o) **"compression"** The coding of data to save storage space or transmission time. Although data is already coded in digital form for computer processing, it can often be coded more efficiently, (using lower bits), utilising the various compression mechanisms, data must be compressed before it can be used.

p) **"relate to business"** All work should and must be of an official nature. Without entity approval, no private work on entity equipment / asset is permitted.

q) **"backup"** The saving of files onto magnetic tapes or other offline mass storage media for the purposes of preventing loss of data in the event of equipment failure or destruction.

r) **"archive"** The saving of old or unused files onto magnetic tapes or other offline mass storage media for the purpose of releasing on –line storage room.

s) **"restore"** The process of bringing off-line storage data back from the offline media and putting it in an online storage system such as a file server.

PART A: INFORMATION TECHNOLOGY

1. PURPOSE

1.1 The aim of this policy is to protect the Board of UGUSCT ("The Entity") information technology infrastructure and related assets against potential abuse. To protect Entity's sensitive information against possible harmful damage and to safeguard the Company against liability as a result of negligent actions caused by its employees through the use of IT infrastructure and related equipment.

2. BACKGROUND

21. UGUSCT values all electronically gathered information as a very important asset in it's daily operations and recognises that Information Technology is a crucial driver to continuously enhance productivity. UGUSCT's vision regarding Information Technology is to achieve an integrated information management system that will eliminate duplication of information as far as is humanly possible.

2.2 In order to achieve this vision, the UGUSCT decided to provide their officials with a network infrastructure that consist of various hardware and software elements. This network infrastructure needs to be effectively maintained in order to protect UGUSCT's investment. The IT policy is applicable to all users of computer related resources.

3. ACCESS TO THE NETWORK

3.1 The Chief Executive Officer will have to select a network, which will be a standard network to be used by the Municipality in line with the supply management policy. The operating system allows users to access these functional applications across the network via a desktop computer/laptop and to share information of common interest with all relevant employees or groups of employees.

3.2 In order to enable effective communication, all users require a user identification/ user name and a password. The passwords need to be frequently changed for security purposes. The sharing of password is strictly prohibited.

4. ACCESS TO FUNCTIONAL APPLICATIONS

4.1 Certain functional applications require a password and enforce the use of passwords to protect the privacy date and malicious utilisation and unauthorised access to official information. The various rules and security procedures as determined by the functional owners (system supervisors/administrator) for the usage of these applications needs to be adhered to.

5. INTERNET

5.1 The Internet and email provided by the Entity is intended for business purposes only. The Entity encourages the use of Internet and e-mail because they make the entity business more efficient and effective. However, the Internet service and e-mail are the property of the entity and the purpose is to facilitate the organisations operations.

5.2 Every employee has the duty and responsibility to maintain and enhance the entity's image and to use the Internet and e-mail access in a productive manner. The relevant head of department should determine at which level are employees entitled to use the e-mail and Internet facilities.

5.3 The Entity prohibits certain categories of access and activity such as; sending, eliciting, downloading or forwarding the following material in any form (including without limitation, photographs, graphics, sound, video, chain letters or text is prohibited):

(i) Material related to illegal activities (including without limitation any material that violates copyright laws)
(ii) Obscene pornographic material;
(iii) Harassing material (including without limitation sexually and racially harassing material);
(iv) Threatening material: material that contains references to an individual's or corporate entities character, competence that are false, are defamatory, would invite contempt and ridicule, with interfere with an existing or potential business relationship; or material that invades another individual's or corporate entities right to piracy (including without limitation surreptitiously reading another's email, disseminating private information, and using a famous name or fact for advertising purpose).
(v) Sending, downloading, or receiving works protected by copyrights (a property right in an original work of authorship, such as software. written work product, graphic works without the permission of the owner of the copyright is prohibited.)
(vi) Sending, downloading or forwarding the proprietary and confidential information of another person or entity without permission.
(vii) Sending cryptography, encryption, and compression, and digital signature software without the prior written approval of the GM: Finance & HR is prohibited. Users who have received such an approval must comply with all applicable export laws, and the user's activity must directly relate to business purpose.
(viii) Users must use caution and judgment when participating on the Internet on work related discussion groups and other public forums. Employees who wish to pursue non- work related Internet activities must do so on their personal time, and must seek their own Internet service providers and establish personal e-mail address.
(ix) A signature that contains an official disclaimer statement will accompany all external e-mail.

6. EXTERNAL COMMUNICATION VIA INTERNET

6.1 Access is granted to certain users to communicate via e-mail. This privilege is primarily granted as a result of the need to cost - effectively communicate, official business related issues on behalf of the entity with the external individuals and organisations.

6.2 Any e-mail correspondence sent over the internet should adhere to the Disclaimer Policy as contained in the attached Disclaimer undertaking and need to be strictly adhered to in order to protect entity's interest at all times.

7. COLLECTING INFORMATION FROM THE INTERNET

7.2 The Internet provides UGUSCT employees with a wealth of information for business use, including research, education and training. The Internet also introduces new risks. The nature of the Internet environments is such that special attention must be focused on issues of entity's image, liability and information security.

7.3 Access to the Internet is provided to UGUSCT employees as an information tool that should be considered an extension/addition to the official business "toolset" of the entuty.

7.4 Usage of the Internet is also monitored and data usage of the internet (log files) is archived for management purposes. All company policies concerning the protection of proprietary information; how we conduct business; how we protect UGUSCT trademarks, logos, and crest; and all other rules and traditions that govern who we are and how we act; are fully relevant to the internet.

7.5 Content development and implementation of the Entity's website is the responsibility of the GM: Marketing & Eventing. All content for Internet pages must be added or revised via the appropriate procedure, through the departmental team and the CEO.

7.6 This IT policy applies to all individuals, (employees, temporary staff etc.) who may use the entity's Information Technology structure or computer related resources. Disciplinary action may be taken against any employee that violates this policy; this policy will be periodically updated or modified as requested.

8. DATA BACKUP

8.1 This policy defines the backup policy for computers within the entity, which are expected to have their data backed up.

(a) Purpose

This policy is designed to protect data in the Entity to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

(b) Scope

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

(c) Timing

Full backups are performed Monthly.

(d) Responsibility

The GM: Finance & HR shall perform regular backups and a system for testing backups and test the ability to restore from backups on monthly basis.

(e) Testing

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

(f) Data Backed Up

Data to be backed up include the following information:

- User data stored on hard drive
- System state data
- The registry
- Financial data

(g) Archives

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

(h) Restoration

Users that need files must submit a request to the GM: Finance &HR.

9. ANTI - VIRUS

9.1 This policy is an internal policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, prevent and remove virus programmes.

9.2 Purpose

(a) This policy is designed to protect the organisational resources against intrusion by viruses.

(b) The organisation will use a single anti-virus product for anti-virus protection that will be determined by the GM: Finance & HR in conjunction with the CEO. The following minimum requirements shall remain in force:

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

(c) No one shall be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

10. INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN

10.1 Introduction

This plan explains the steps to restore Information Technology services if any 'disaster' disables any of South Coast Tourism Information Technology equipment.
The steps taken to preserve key data in the advent of a 'disaster' are also included in this document.

A disaster includes events like fires, natural disasters, riots. It also includes malicious viruses, hacking or any activity that stops the normal working of the systems.

10.2 Scope

All equipment and services supplied by South Coast Tourism. This includes are servers and Computers with their related programs and data.

10.3 Data Backups

All official South Coast Tourism critical data are backup on an external device as per the Information Technology Policy and Procedure document. Thus only data backups of critical information are required.
There are currently eight Computers in use at South Coast Tourism. Below are the details on how we currently backup the Computers:

Machines	LOCATION	BACKUP DETAILS	Monthly BACKUP TIME
CEO	Head Office	All data and E-Mail	15:30 pm
Admin	Head Office	All data and E-Mail	15:30 pm
Development	Head Office	All data	15:30 pm
Marketing	Head Office	All data	15:30 pm
Events	Head Office	All data	15:30 pm
Membership	Head Office	All data	15:30 pm
Info	Head Office	All data	15:30 pm
Accounts	Head Office	All data	15:30 pm

In the event of a disaster at South Coast Tourism the following Recovery procedure will be carried out:

Below is a checklist of all the points that will be carried out in the event of a disaster at our Head Office: For example, "South Coast Tourism Office burns down due to an electrical short and all the computers are damaged including Servers. "

1. Move all working equipment to the Margate offices.
2. Relocate all users from Head Office in available offices, Training centre and Board Room.
3. Purchase Additional Computer Equipment (If needed): Components that need to be replaced will be replaced by a Computer Retailer. These components will be installed within the agreed Turnaround time between South Coast Tourism and the retailer.(See Appendix A, Copy of the Agreed Turnaround time for the replacement of Servers and Other Computer Equipment with the Retailer.)
4. Install New Servers and computers, including software, network and restore last Monthly backup.(If needed)
5. Install New Computers, software connect to Network. (If needed).

Listed below is a table estimated the turnaround time after a disaster at South Coast Tourism

EQUIPMENTS	RELOAD SOFTWARE	OBTAIN HARDWARE	RELOCATE HARDWARE AND SETUP CABLING/HUBS
Printers	30min	4hrs	4hrs
Routers and Switches	30min	4hrs	2hrs
Computers	5hrs	5hrs	4hrs

PART B: COMMUNICATION

1. INTERNAL COMMUNICATION

The Entity realises that sound labour relations can only result from mutual respect between an employer and its employees and that such respect is formed where the employer and its employees treat each other fairly and consistently. This policy is designed to achieve the aim of sound labour relations in an open and fair work environment and to ensure that information dissemination strategies are effective.

1.1 **Workplace Communication**

The Entity believes that the channels of communication must exist between management and its employees in every workplace.

1.2 **Appointments with management and Board Members**

(i) An employee, except departmental head, and a person working in his/her office, must make an appointment to consult the CEO. The employee making an appointment must indicate the subject matter that he/she wishes to raise.

(ii) An employee, except a departmental head working directly under the supervision of a departmental head, must make an appointment to consult his/her departmental head. The employee making the appointment must indicate the subject matter he/she wishes to discuss.

(iii) No employee, except a departmental head, makes an appointment with the CEO, without the prior permission of his/her departmental head. The employee who wishes to make such an appointment must indicate the subject matter that he/she wishes to raise with the CEO, to his/her departmental head.

(iv) No employee may make an appointment with his/her, or another departmental head without the prior permission of his/her immediate supervisor.

(v) Subject to paragraph (vii), no employee other than the CEO or departmental head may make an appointment with the Chairman or any other Board member.

(vi) The Chair may summons any employee to consult with him/her, but such employee must report the fact that he/she has been summonsed to his/her departmental head.

(vii) A trade union has the right to make an appointment with the CEO, or a departmental head to discuss a matter of mutual concern relating to the Entity or a specific department or a workplace within a department. The trade union making the appointment must state the subject matter that it wishes to raise.

(viii) Notwithstanding the provision of paragraph (v), an employee may make an appointment with a Board member in order to make a protected disclosure to that Board Member in terms of the Protected Disclosures Act.

(ix) Whenever an employee approaches a Board Member, except in the circumstances contemplated in paragraph (viii), that Board Member must advise the employee concerned to follow the correct procedure to bring the matter he/she raised with the Board Member to the attention of the CEO or another employee.

2. EXTERNAL COMMUNICATION

2.1 Objective

2.1.1 The objective of this policy is to ensure that the organisations handle relationships with its stakeholders in a professional and consistent manner and that there is a proper record of same.

2.2 Communication with stakeholders

2.2.1 Both the CEO and/or the Chairman are responsible for communicating with all stakeholders of the Entity. All information that is sent by the organisation needs to be sanctioned by the CEO and/or the Chairman.

2.2.2 The following should be noted:

i) No employee should deal directly with the government, or any of the Entity's key stakeholders without prior consultation and support of the CEO and/or Chairman.
ii) If an employee is approached by any of the stakeholders, they must refer them to the CEO and/or the Chairman.
iii) It is totally inappropriate and unacceptable for an employee to make any public statements or speculate on any subject that has to do with the Entity's operations. All external enquiries from the stakeholders and the media need to be referred to the CEO and /or the Chairman and;
iv) Employees should strictly adhere to this policy. Any contravention by employees of any of the above may/will result in disciplinary action.

3. CEO / AREA CHAIRS FORUM

The Entity should consist of a CEO / Area Chairs Forum, which will ensure that all strategic decisions relating to communication are taken.

3.1 OBJECTIVES OF THE COMMUNICATION FORUM

3.1.1 An integrated Communication, providing for:

i) Sharing of information across different organisations, departments and other relevant stakeholders.
ii) Identification of opportunities of co-operation and teamwork.
iii) Making the most of shared opportunities and assets
iv) Common understanding across all stakeholders of the Entity.

3.2 **A COMMUNICATION FORUM WITH MECHANISMS FOR**:

i) Development of regular communication to stakeholders of the Entity
ii) Integrated strategies where integrated messages, priorities and themes through the voice of the CEO are involved
iii) Integrated approaches and Communication actions
iv) Achievement of "one voice" where possible i.e both to maximise positive issues and minimise negative issues
v) Monitoring and evaluation of the communication actions that are generated as part of the forum
vi) Annual reporting and performance reporting
vii) Intergovernmental relations

3.3 **INFORMATION SHARING: INTER, INTRA AND EXTRA DEPARTMENT/ ORGANISATION**

i) Improving the knowledge base internally and externally
ii) Making the connection between the issues of different wards, departments and regions
iii) Learning forum ensuring that meetings are an opportunity to learn about policies, strategies and interventions of, and affecting different wards and departments.

4. RESPONSIBILITY FOR THE COMMUNICATION POLICY

4.1.1 The Management Team

4.1.2 The CEO and GM's should be responsible for driving the Communication Policy including Area Chair Committee Policy by actively and demonstrably, applying it's principles to all aspects of their work.

4.1.3 They should:

i) Communicate their decisions, and the strategic thinking behind them, clearly and expeditiously to the stakeholders so that cascading of essential information to staff at all levels can be instigated (where appropriate) in an accurate and timely manner

4.1.2 The General Managers

4.1.2.1 All the GM's should take particular responsibility for ensuring the successful implementation of this policy within their areas of responsibility.

4.1.2.2 They should:

i) Ensure that all staff members are fully aware of the Communication Policy including Area Committee Policy and are acting upon it.
ii) Provide regular feedback to their own CEO through the Management team meetings, thus creating an upward flow of information as well as the usual "top – down" procedure
iii) Provide information to, and liaise with, elected members within the guidelines of the established protocol.

iv) Establish channels of communication for staff to express their views and opinions on internal procedures, policies and practices.
v) Provide regular feedback to the CEO through the established Communication Forum.
i) Advise and recommend on future planning on Communication issues.

4.2 Area Committees

4.2.1 The Area Committees as the form of communication should be responsible for making sure that the communities are involved and informed about Board decisions that affect their areas.

4.2.2 They should:

i) Advise CEO on development and other projects in the ward
ii) Play a role in informing communities of entity plans, programmes and decisions so as to ensure transparency.
iii) Deal with all matters that affect and benefit the community.
iv) Make recommendations to the Board on any matter affecting the areas.
v) When area committees call public meetings, that need media or other methods of communicating, the Entity should provide the financial support.

5. COMMUNICATION VEHICLES

5.1 The Entity should implement the following communication vehicles in order to have an efficient and effective communication channel that will always promote transparency and unity.

i) Official written communication vehicles

- *Newsletters*
- *Local Newspapers*
- *Memos*
- *Pamphlets*
- *Annual Report & Performance Report*
- *Letters*

ii) Electronic Communication Vehicles

- *Radio Stations*
- *Email*
- *Telephone, cellphones and faxes*
- *Videos*
- *Projectors*
- *Website*

iii) Other Communication vehicles

- *Notice boards*
- *Public meetings*

iv) Area Committees (as communication vehicles)

5.2 Area committees are mainly advisory committees, which can make recommendations on any matter affecting the ward.

(a) **Conduct of Area Committee members**

A Area Committee member will abide by the following:-

- Perform the functions of the committee in good faith and without or prejudice
- May not use it's position or privileges for personal gain or to improperly benefit another person
- Accept the principle of accountability to the community
- Not compromise the credibility and integrity of the committee
- Function in support of the Area Chair and Entity
- Be accessible to the community
- Ensure transparency and openness in the operations of the committee
- Ensure that all views and opinions are considered
- Be punctual for meetings and must submit an apology to the Chairperson in advance if a meeting cannot be attended.