		IQA Policy P34	
National Secretariat		**IT Data storage, email & password policy**	
Policy Number:	P17-34	**Version:**	01
Date Adopted:	16/10/13	**Contact:**	Company Secretary

1. Data Storage

1.1. Overview

The cloud storage in use by the IQA is a service provided by box.com. This system allows access to files from any location that has internet access and an internet browser supported by Box. Supported browsers included:

- Internet Explorer
  - IE8, IE9, and IE10 are fully supported (excepting Box Notes)
  - Box Notes (Beta) is only supported on IE10
- Safari (Latest version)
- Firefox (Latest version)
- Google Chrome (Latest version)

Box is also available on many mobile devices such as Android and iOS. The main way of staying up to date however is through the use of the Box Sync for Windows/Mac.

1.2. Purpose

The IQA is responsible for securely storing all computer files that employees, contractors and outside agencies require access to. Any attempt to violate the provisions of this policy may result in disciplinary action in the form of revoking user access, or application of the IQA's performance management system.

1.3. Scope

The scope of this policy applies to all employees/contractors that have access to the cloud storage service.

1.4. Policy

1.4.1.Storage Limitations

The total amount of storage available to the IQA is 1TB. Thus no user will exceed 100GB in personal (work related) storage.

1.4.2.Personal Use of Cloud Storage

Personal use of the cloud storage is not allowed by employees or contractors.

1.4.3.Prohibited Access

- **Use of Files** - deletion, examination, copying, or modification of files and/or data belonging to other users without their prior consent is prohibited.
- **Use of cloud storage system** - use of facilities and/or services for non IQA commercial purposes is prohibited.
- **Unauthorised Use** - any unauthorised, deliberate action that damages or disrupts the system, alters its normal performance, or causes it to malfunction is a violation regardless of system location or time duration.

- **Music and/or Video files -** that are not work related are not to be stored on this service under any circumstances. If found they will be deleted without notice and will not be restored under any circumstances.

2. Email System

2.1. Overview

Email is a very important method of the communication in the current time for our organization. But users should understand that incorrect use of the email system may be very dangerous for both the users and the Institute (legal reasons: sexual harassment, for example, and technological reasons: email often becomes the way for penetration of the viruses in the Institute's network). So, all users (including contractors with access to the Institute's email system) are responsible for taking the appropriate steps, as outlined below, to correctly use the Institutute email system.

2.2. Purpose

The purpose of this policy is to ensure the proper use of the IQA's (Institute) email system and make sure users are aware of what the Institute deems to be acceptable and unacceptable use of its email.

2.3. Scope

The scope of this policy includes all personnel who have or are responsible for access to the Institute email system.

2.4. Policy

2.4.1. Mail Box Limits

- A limit of 30GB applies to all emails.

Remember to clean out and archive emails on a regular basis to prevent reaching this limit.

2.4.2. Prohibited Use

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- If a user sends or forwards an email with any libellous, defamatory, offensive, racist or obscene remarks, the user and the Institute can be held liable.
- If a user unlawfully forwards confidential information, the user and the Institute can be held liable.
- If a user unlawfully forwards or copies a message without permission, the users and the Institute can be held liable for copyright infringement.
- If a user sends an attachment that contains a virus, the user and the Institute can be held liable.

By following this policy, the user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this email policy, the user will be fully liable.

The following rules are required by law and are to be strictly adhered to.
It is prohibited to:

- Send or forward emails containing offensive or disruptive content, which includes, but is not limited to defamatory, offensive, racist or obscene remarks. If a user receives an email of this nature, your Branch Chairperson or the General Manager must be promptly notified.

- Forward a message without acquiring permission from the sender first.
- Send unsolicited email messages.
- Forge or attempt to forge email messages.
- Disguise or attempt to disguise identity when sending mail.
- Send email messages using another person's email account.
- Copy a message or attachment belonging to another user without permission of the originator.

2.4.3. Personal Use.

No personal use of the Institutes email system is permissable.

2.4.4. Monitoring

Institute employees and contractors shall have no expectation of privacy in anything they store, send or receive on the Institute's email system. The Institute may monitor messages without prior notice. The Institute is not obliged to monitor email messages.

2.4.5. Disclaimer

Make sure that your email signature has this disclaimer at the bottom of it:

Please do not print this email unless you really need to.
This communication is confidential and may also be legally privileged. If you are not the intended recipient, please notify us immediately via reply to this email address and delete/ destroy all copies. If you are not the intended recipient you should not copy this email, disseminate it, disclose its contents to another person, or use it for any other purpose. No warranty is made that the email or attachment(s) are free from computer virus or other defect.

2.4.6. Confidential Information

Never send any confidential information via email. If the user is in doubt as to whether to send certain information via email, check this with the General Manager first.

2.4.7. Privacy

Employees are given email access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, send or receive using the Institute's services. These services are purchased by the Institute and may be used only for Institute purposes.

The Institute reserves the right to monitor employee use of the Institute email system.

Subject to approval from the General Manager or Company Secretary, the Institute may access and disclose the contents of emails and/or files.

2.5. Best Practices

The Institute considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an email as they would for any other communication. Therefore the Institute wishes users to adhere to the following guidelines:

2.5.1. Writing emails:

- Write well-structured emails and use short, descriptive subjects.
- The Institute's email style is informal. This means that sentences can be short and to the point. Start the email with 'Hi', or 'Dear', and/or the name of the person. Messages can be ended with 'Best Regards'. The use of Internet abbreviations and characters such as smiles (☺) however, is not encouraged.
- Signatures must include the sender's name, job title and Institute name, contact details and the relevant information for the next national conference.
- Users must spell check all mails prior to transmission.
- Do not send unnecessary attachments.
- Do not write emails in capitals.
- If a user forwards an email, clearly state what action the recipient is to take.
- Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
- Only mark emails as important if they really are important.

2.5.2. Spam and viruses in emails:

- If a user receives an email with an unsolicited message (advertising about services or products), it is recommended that you remove it from your computer. Be careful not to leave the Institute email address in the news-groups, forums, or filled in the forms on Internet sites (lotteries, competitions and so on).
- If a user receives an email with an attachment, which is not expected – just delete it. A lot of viruses are distributed in such a way. New viruses are distributed with attachments in the ".zip" archives with password in the body of the letter – do not try to open such archives.
- If a user has any doubts, ask the IT department for recommendations – it is better to prevent the penetration of a new virus in our network than cure it.

2.5.3. Maintenance

- Delete any email messages that are not required any more; empty your 'deleted items' folder, as a minimum, once a month.

3. Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Institutes entire network. As such, all Institutes employees (including contractors with access to the Institutes network) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.1. Purpose

The purpose of this policy is to establish a standard for creation of Strong Passwords, the protection of those passwords, and the frequency of change.

3.2. Definition

Strong Password – a password that has upper and lower case characters, numbers and is at least eight characters in length as a mimumum.

3.3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Institute site, has access to the Institute's network, or stores any non-public Institute information.

3.4. General Policy

- Details of the password policy for the IQA domain:
- Minimum password length: 8 characters
- Users must log on in order to change password.
- A copy of all Admin and Systems Account passwords should be kept by the IT Contractor in a secured location.
- All user-level and system-level passwords must conform to the guidelines described below.

3.5. Guidelines

Passwords are used for various purposes. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection and local router logins.

Poor or weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family members, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Strong passwords have the following characteristics:
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least six characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrases.
- NOTE: Do not use either of these examples as passwords!

3.6. Password Protection Standards

Do not use the same password for Institute accounts as for other non-Institute access (e.g. personal ISP account, etc.). Where possible, don't use the same password for various Institutes' access needs. For example, select one password for the Membership systems and a separate password for IT systems. Do not share Institute passwords with anyone.

All passwords are to be treated as sensitive, confidential Institute information. Here is a list of dont's:

- Don't reveal a password over the phone to ANYONE.

- Don't reveal a password in an email message.
- Don't reveal a password to your supervisor or manager.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g. my family name).
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on holiday or away from the office.

If someone demands a password, refer them to this document or have them call someone in the IT department.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including mobile or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to the IT department and change all passwords.

I ________________________ hereby acknowledge that I have read and fully understand the aforementioned IT data storage, email and password IQA Policy 17 – P34 and agree to abide the by contents of same. Violation of the provisions of this policy may result in disciplinary action in the form of revoking user access, or application of the IQA's performance management system.

--------------------------------------   ----- / ----- / ------
Signed   Date