POLICY

INFORMATION SECURITY GDPR

Version 3.1

01904 310 272 | info@catalyst-it.co.uk | catalyst-it.co.uk

CATALYST IT
ACCELERATING BUSINESS PERFORMANCE

Document control

Version History

Version	Date	Comments
Draft 0.1	**02/05/2014**	**First draft by Lee Connor Technical Director**
Draft 0.2	**24/06/2014**	**Amends by Richard Grierson**
Final 1.0	**30/06/2014**	**Clean Desk Policy added by Lee Connor**
Final 1.1	**10/07/2014**	**Anti-Virus Guidelines added by Lee Connor**
Final 1.2	**03/09/2014**	**Software Installation Policy added by Lee Connor**
Final 2.0	**26/02/2015**	**Web Application Security Policy added by Lee Connor**
Final 2.1	**17/03/2015**	**Bring Your Own Device Policy added by Richard Grierson**
Final 2.2	**18/03/2015**	**Text amends by Richard Grierson**
Final 2.3	**05/05/2015**	**Added internet connection Guidelines**
Final 3.0	**24/02/2018**	**GDPR Additional Measures added**
Final 3.1	**22/11/2018**	**Text Changes to omit errors**
Final 3.2	**05/02/2020**	**Formatting updates**
Final 3.1	**17/03/2021**	**New Template Format**

Issue Control

Author:	Lee Connor
Owner and approver:	**Catalyst IT Directors**

Table of Contents

Data protection policy

Overview:

This policy describes how personal data must be collected, handled and stored to meet the company's data protection standards, protecting customer and Catalyst Data and ensuring all employees comply with the law.

Purpose:

This data protection policy ensures Catalyst IT:

- Complies with data protection law, GDPR and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law:

The Data Protection Act 1998 describes how organisations — including Catalyst IT— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

General Data Protection Regulation:

The General Data Protection Regulation (GDPR) enhances the Data protection law and contains many requirements about collecting, storing and using personal information, including:

- Identify and secure the personal data in our systems
- Accommodate new transparency requirements
- Detect and report personal data breaches
- Train privacy personnel and other employees

All EU companies need to be GDPR compliant as of May 2018, this will ensure that all data including personal data is handled with due care and attention by all employees of Catalyst.

Under GDPR, the data protection principles set out the main responsibilities for organisations and requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. The controller (or Catalyst personnel) shall be responsible for, and be able to demonstrate, compliance with the principles.

Scope:

This policy applies to:

1. The head office of Catalyst IT
2. All staff and volunteers of Catalyst IT
3. All contractors, suppliers and other people working on behalf of Catalyst IT

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

1. Names of individuals
2. Postal addresses
3. Email addresses
4. Telephone numbers
5. …plus any other information relating to individuals

Data protection risks:

This policy helps to protect Catalyst IT from some very real data security risks, including:

- **Breaches** of confidentiality. For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage**. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities:

Everyone who works for or with Catalyst IT has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility: The board of directors is ultimately responsible for ensuring that Catalyst IT meets its legal obligations.

The **Technical Director** is responsible for:

1. Keeping the board updated about data protection responsibilities, risks and issues.
2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
3. Arranging data protection training and advice for the people covered by this policy.
4. Handling data protection questions from staff and anyone else covered by this policy.
5. Dealing with requests from individuals to see the data Catalyst IT holds about them (also called 'subject access requests').
6. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
7. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
8. Ensure regular checks and scans to ensure security hardware and software is functioning properly.
9. Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The **Sales and Marketing Director**, is responsible for:

1. Approving any data protection statements attached to communications such as emails and letters.
2. Addressing any data protection queries from journalists or media outlets like newspapers.
3. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines:

1. The only people able to access data covered by this policy should be those who need it for their work.
2. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
3. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
4. In particular, strong passwords must be used, and they should never be shared.
5. Personal data should not be disclosed to unauthorised people, either within the company or externally.
6. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
7. Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data Accuracy:

The law requires Catalyst IT to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater the effort Catalyst IT should put into ensuring its accuracy.

1. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
2. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
3. Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
4. Catalyst IT will make it easy for data subjects to update the information Catalyst IT holds about them. For instance, via the company website.
5. Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
6. It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests:

All individuals who are the subject of personal data held by Catalyst IT are entitled to:

1. Ask what information the company holds about them and why.
2. Ask how to gain access to it.
3. Be informed how to keep it up to date.
4. Be informed how the company is meeting its data protection obligations.

If an individual contact the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Protection Steward at DPS@catalystitsolutions.co.uk

The data steward will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons:

In certain circumstances, the Data Protection Act and GDPR compliance allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Catalyst IT will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information:

Catalyst IT aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

Policy Compliance:

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Catalyst IT team in advance.

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

Data Handling Guidelines

GDPR requires personal data to be processed in a manner that ensures its secure, this includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The following policies identify how to minimise this impact during data handling process.

Personal Data Handling:
The data is deemed to be of a personal nature if the person can be identified in any way i.e. this includes data such as:

- Name
- Email Address
- Telephone number
- Identification number
- Location data
- Online identifier

Data can be identified as personal even if the data is pseudonymised e.g. key-coded depending on how the coding has been achieved for example this can including:

- Initials
- First name Letter & Surname

Sensitive personal data:
Catalyst will not handle, process any data that is deemed to the sensitive, sensitive is deemed to be special categories of personal data, such as:

- Genetic
- Biometric
- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Health
- Sex life
- Sexual orientation

Personal data relating to criminal convictions and offences are not included in this, however, Catalyst will also not process this data.

Data Use:
Personal data is of no value to Catalyst IT unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

1. When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
2. Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
3. Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
4. Personal data should never be transferred outside of the European Economic Area.

5. Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Collection:
Data must be collected in a fair manor, fair being that the individual understands why the data is being collected and it use. Any data Catalyst collects directly will need be logged in the Data Audit log. Identifying when, how and reason the data was collected.

Data Consent:
Data collected by Catalyst staff (or the suppliers of data to Catalyst) will need consent from the individual for the data to be used. This ensures the evidence needed to comply with GDPR but also gives the individual the opportunity to reject or challenge the use of their information.

This covers the use of emailers from Catalyst data sets and we must:

- Have made the request for consent prominent and separate from our terms and conditions
- Asked to positively 'opt in' with no default tick boxes
- Use clear, plain language that is easy to understand
- Specify why we want the data and what we're going to do with it
- Give individual ('granular') options to consent separately to different purposes and types of processing
- Name our organisation and any third party controllers who will be relying on the consent
- Ensure we inform the individuals they can withdraw their consent and the process of this

This means that all personal data collected will need to have evidenced constant and controlled via the following:

- Logging the consent within NetSuite (Catalysts internal ERP solution) which consists of the opt-in type in: Contact → Marketing → Subscriptions
- All email-shots have an opt-out option
- All initial opt-in options have multiple options consisting of:
    - Billing Communication
    - Events
    - NetSuite Marketing
    - Newsletters
    - Product Updates
    - Qlik Marketing
    - Surveys
- No communications, electronic or otherwise are sent to contacts that have not explicitly opted in

Withdraw of Consent:
Our ERP solutions will be the master source of opt-in and therefore withdrawals will be made via the same system. Either a manual or automated request via an e-shot will be replicated into NetSuite.

It is up to the processor of automated email's to ensure all automated withdrawals are correctly processed from the email solution into

International Transfers:
Any data being transferred out of the EU contravenes GDPR regulations and as such Catalyst employees will not send any data to any country outside of the EU or to any recipient that the end country is not known.

Customer and Supplier Transfers:
Data transfer to third party suppliers or from customer must be secured using secured process as identified in the Data Audit process.

Policy Compliance:

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Catalyst IT team in advance.

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

Data Audit Guidelines & Process

Data Audit:
All data being stored by Catalyst IT must be passed through the data audit and logging process which the Data Protection Steward administrates.

- Before any data is accepted by any employee on any media (email, USB, FTP, download etc) they must notify the data protection steward
- All data before processing must be audited and a DPIA performed
- Once data sources are approved processing can be performed
- Data must be destroyed as per instructions from the data audit

All data must be handled as per Data Handling Guidelines and must be assumed it is of a personal nature, Data will not be handled and must be refused if the data is defined as sensitive.

Data protection impact assessments (DPIAs):

Data protection impact assessments is a tool which identify the most effective way to deal with their data obligations and meet individuals' expectations of privacy.

The DPIA will be completed on acceptance of all data in the first instance, this process alone will identify the data as personal or not.

1. The DPIA will identify the following and will augment this policy focused on:
2. Identify if the data is personal or of a sensitive nature
3. Identification of the information flow and any associated personal data risks
4. Ensure that storage and processing is necessary
5. Ensure consultation with external concerned parties (Customer, Suppliers and even the individuals identified in the data)
6. Provide any privacy solutions for the data in question
7. Provide the process of how to handle the data
8. Identify the need and timescales for data destruction
9. Ensure both the breach detection and notification process is aligned with the data in question

Policy Compliance:

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Catalyst IT team in advance.

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

Policy Compliance:

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Catalyst IT team in advance.

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

Data Breach Guidelines

GDPR introduces a duty on all Catalyst to report personal data breaches to a supervisory authority. Catalyst must do this within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

Detection:
A breach is defined as:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

Breach Recording:
Catalyst must also keep a record of any data breaches weather these are validated or not breeches, this must be done immediately, and an email send to Catalysts 'Data Protection Steward' at the following email address

- DPS@catalystitsolutions.co.uk

Policy Compliance:

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Catalyst IT team in advance.

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

Password Construction Guidelines

Overview:
Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Catalyst network. This guideline provides best practices for creating secure passwords.

Purpose:
The purpose of this guidelines is to provide best practices for the created of strong passwords.

Scope:
This guideline applies to employees, contractors, consultants, temporary and other workers at Catalyst, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Statement of Guidelines:
All passwords should meet or exceed the following guidelines

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, syxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

We should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.
(NOTE: Do not use either of these examples as passwords!)

Passphrases:
Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper

and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

Policy Compliance:

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Catalyst IT team in advance.

Non-Compliance

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

Password Protection Policy

Overview:
Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorised access and/or exploitation of Catalyst IT's resources. All users, including contractors and vendors with access to Catalyst IT systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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.

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 Catalyst IT facility, has access to the Catalyst IT network, or stores any non-public Catalyst IT information.

Password Creation:

1. All user-level and system-level passwords must conform to the Password Construction Guidelines.
2. Users must not use the same password for Catalyst IT accounts as for other non-Catalyst IT access (for example, personal ISP account, option trading, benefits, and so on).
3. Where possible, users must not use the same password for various Catalyst IT access needs.
4. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
5. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

Password Change:

1. All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
2. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
3. Password cracking or guessing may be performed on a periodic or random basis by the Catalyst IT Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Password Protection:

1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential Catalyst IT information. Corporate Information Security recognises that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
2. Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

3. Passwords must not be revealed over the phone to anyone.
4. Do not reveal a password on questionnaires or security forms.
5. Do not hint at the format of a password (for example, "my family name").
6. Do not share Catalyst IT passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
8. Do not use the "Remember Password" feature of applications (for example, web browsers).
9. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Application Development:

Application developers must ensure that their programs contain the following security precautions:

1. Applications must support authentication of individual users, not groups.
2. Applications must not store passwords in clear text or in any easily reversible form.
3. Applications must not transmit passwords in clear text over the network.
4. Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Use of Passwords and Passphrases:

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The?#>*@TrafficOnThe101Was*&#!#ThisMorning"*

All of the rules above that apply to passwords apply to passphrases.

Password Saving:

Current Microsoft Windows and associated applications allow the storing of passwords when using remote desktop, browsers, SQL connections etc.

All storage of corporate, customer or supplier passwords is not permitted to be enabled unless they are one of the following exceptions:

- Outlook
- Skype for Business

Centralised Password Storage:
As the Catalyst team need to store and potential share passwords for multiple clients and projects Catalyst utilise a Password Management Tool. Passwords are not stored by Browsers.

Policy Compliance:

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Catalyst IT Team in advance.

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

Acceptable Use Policy

Overview:
Catalyst IT's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Catalyst IT's established culture of openness, trust and integrity. Catalyst IT is committed to protecting Catalyst IT's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Catalyst IT.

These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Catalyst IT employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose:
The purpose of this policy is to outline the acceptable use of computer equipment at Catalyst IT. These rules are in place to protect the employee and Catalyst IT. Inappropriate use exposes Catalyst IT to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope:
This policy applies to the use of information, electronic and computing devices, and network resources to conduct Catalyst IT business or interact with internal networks and business systems, whether owned or leased by Catalyst IT, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Catalyst IT and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Catalyst IT policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Catalyst IT, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Catalyst IT.

General Use and Ownership:

1. Catalyst IT proprietary information stored on electronic and computing devices whether owned or leased by Catalyst IT, the employee or a third party, remains the sole property of Catalyst IT. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*
2. You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Catalyst IT proprietary information.
3. You may access, use or share Catalyst IT proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.
4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on

personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
5. For security and network maintenance purposes, authorised individuals within Catalyst IT may monitor equipment, systems and network traffic at any time, per Catalyst IT's *Audit Policy*.
6. Catalyst IT reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information:

1. *All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.*
2. *System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.*
3. *All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.*
4. *Postings by employees from a Catalyst IT email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Catalyst IT, unless posting is in the course of business duties.*
5. *Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.*

Unacceptable Use:

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Catalyst IT authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Catalyst IT-owned resources.
The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities:

1. The following activities are strictly prohibited, with no exceptions:
2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Catalyst IT.
3. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Catalyst IT or the end user does not have an active license is strictly prohibited.
4. Accessing data, a server or an account for any purpose other than conducting Catalyst IT business, even if you have authorised access, is prohibited.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a Catalyst IT computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Making fraudulent offers of products, items, or services originating from any Catalyst IT account.
10. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
11. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Port scanning or security scanning is expressly prohibited unless prior notification to Catalyst IT is made.
13. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
14. Circumventing user authentication or security of any host, network or account.
15. Introducing honeypots, honeynets, or similar technology on the Catalyst IT network.
16. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
17. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
18. Providing information about, or lists of, Catalyst IT employees to parties outside Catalyst IT.

Email and Communication Activities:
When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that “the opinions expressed are my own and not necessarily those of the company”. Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorised use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.
5. Creating or forwarding “chain letters”, “Ponsi” or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within Catalyst IT’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Catalyst IT or connected via Catalyst IT’s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media:

1. Blogging by employees, whether using Catalyst IT's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Catalyst IT's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Catalyst IT's policy, is not detrimental to Catalyst IT's best interests, and does not interfere with an employee's regular work duties. Blogging from Catalyst IT's systems is also subject to monitoring.

2. Catalyst IT's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Catalyst IT confidential or proprietary information, trade secrets or any other material covered by Catalyst IT's Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Catalyst IT and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Catalyst IT's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to Catalyst IT when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Catalyst IT. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Catalyst IT's trademarks, logos and any other Catalyst IT intellectual property may also not be used in connection with any blogging activity.

Policy Compliance

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Catalyst IT team in advance.

Non-Compliance

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

Clean Desk Policy

Overview
A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilise when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

Purpose
The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

Scope
This policy applies to all Catalyst IT employees and affiliates.

Policy

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the work day.
4. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
5. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
6. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
7. Laptops must be either locked with a locking cable or locked away in a drawer.
8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
10. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
11. Whiteboards containing Restricted and/or Sensitive information should be erased.
12. Lock away portable computing devices such as laptops and tablets.
13. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Policy Compliance

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Catalyst IT team in advance.

Non-Compliance

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

Disaster Recovery Plan Policy

Overview
Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realise that having a contingency plan in the event of a disaster gives Catalyst IT a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

Purpose
This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by Catalyst IT that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

Scope
This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

Contingency Plans
The following contingency plans must be created:

1. Computer Emergency Response Plan: Who is to be contacted, when, and how What immediate actions must be taken in the event of certain occurrences
2. Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
3. Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
4. Criticality of Service List: List all the services provided and their order of importance.
5. It also explains the order of recovery in both short-term and long-term timeframes.
6. Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
7. Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
8. Mass Media Management: Who is in charge of giving information to the mass media
9. Also provide some guidelines on what data is appropriate to be provided.

Management will set aside time to test implementation of the disaster recovery plan. Table top exercises will be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

Policy Compliance

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the Technical Director in advance.

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

Remote Access Policy

Purpose
The purpose of this policy is to define standards for connecting to Catalyst IT's network or cloud locations from any host. These standards are designed to minimise the potential exposure to Catalyst IT from damages which may result from unauthorised use of Catalyst IT resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Catalyst IT internal systems, etc.

Scope
This policy applies to all Catalyst IT employees, contractors, vendors and agents with a Catalyst IT-owned or personally-owned computer or workstation used to connect to the Catalyst IT network or within Catalyst IT's or Customers hosted or cloud servers.

This policy applies to remote access connections used to do work on behalf of Catalyst IT, including reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to DSL, VPN, SSH.

Policy
It is the responsibility of Catalyst IT employees, contractors, vendors and agents with remote access privileges to Catalyst IT's corporate or cloud network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Catalyst IT.

General access to the Internet for recreational use by immediate household members through the Catalyst IT Network on personal computers is permitted. The Catalyst IT employee is responsible to ensure the family member does not violate any Catalyst IT policies, does not perform illegal activities, and does not use the access for outside business interests. The Catalyst IT employee bears responsibility for the consequences should the access be misused.

Requirements
1. At no time should any Catalyst IT employee provide their login or email password to anyone, not even family members.
2. Catalyst IT employees and contractors with remote access privileges must ensure that their Catalyst IT-owned or personal computer or workstation, which is remotely connected to Catalyst IT's corporate or hosted network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

3. Catalyst IT employees and contractors with remote access privileges to Catalyst IT's corporate network must not use non-Catalyst IT email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Catalyst IT business, thereby ensuring that official business is never confused with personal business.
4. Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time.
5. Non-standard hardware configurations must be approved by Remote Access Services, and IT must approve security configurations for access to hardware.
6. All hosts that are connected to Catalyst IT internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
7. Personal equipment that is used to connect to Catalyst IT's networks must meet the requirements of Catalyst IT-owned equipment for remote access.
8. Organisations or individuals who wish to implement non-standard Remote Access solutions to the Catalyst IT production network must obtain prior approval from Remote Access Services and IT.

Policy Compliance

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the IT Team in advance.

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

Remote Desktop Policy

Overview
Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa.

Examples of such software include LogMeIn, Join.me, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Catalyst IT network that can be used for theft of, unauthorised access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on Catalyst IT computer systems.

Purpose
This policy defines the requirements for remote access tools used at Catalyst IT

Scope
This policy applies to all remote access where either end of the communication terminates at a Catalyst IT computer asset

Policy
All remote access tools used to communicate between Catalyst IT assets and other systems must comply with the following policy requirements.

Remote Access Tools
Catalyst IT provides mechanisms to collaborate between internal users, with external partners, and from non-Catalyst IT systems. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

1. All remote access tools or systems that allow communication to Catalyst IT resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
2. The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
3. Remote access tools must support the Catalyst IT application layer proxy rather than direct connections through the perimeter firewall(s).
4. Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Catalyst IT network encryption protocols policy.
5. All Catalyst IT antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

Policy Compliance

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the IT Team in advance.

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

Server Security Policy

Overview
Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Catalyst IT. Effective implementation of this policy will minimise unauthorised access to Catalyst IT proprietary information and technology.

Scope
All employees, contractors, consultants, temporary and other workers must adhere to this policy. This policy applies to server equipment that is owned, operated, leased or registered by Catalyst IT.

Policy
All internal servers deployed at Catalyst IT must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by IT.

Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by IT.

The following items must be met:

1. Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
2. Server contact(s) and location, and a backup contact
3. Hardware and Operating System/Version
4. Main functions and applications, if applicable
5. Information in the corporate enterprise management system must be kept up-to-date.
6. Configuration changes for production servers must follow the appropriate change management procedures
7. For security, compliance, and maintenance purposes, authorised personnel may monitor and audit equipment, systems, processes, and network traffic.

Configuration Requirements

1. Operating System configuration should be in accordance with approved IT guidelines.
2. Services and applications that will not be used must be disabled where practical.
3. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
6. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
7. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
8. Servers should be located in an access-controlled environment.
9. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Backups & Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails for physical located servers saved as follows, for all other cloud or virtual servers will be provide by the hosting supplier.

1. All security related logs will be kept online for a minimum of 1 week.
2. Daily incremental backups will be retained for at least 1 month.
3. Weekly backups of logs will be retained for at least 1 month.
4. Monthly full backups will be retained for a minimum of 1 year.

Security-related events will be reported to IT, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

1. Port-scan attacks
2. Evidence of unauthorised access to privileged accounts
3. Anomalous occurrences that are not related to specific applications on the host.

Policy Compliance

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT team in advance.

Non-Compliance

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

Anti-Virus Guidelines

Recommended processes to prevent virus problems:

1. Always run the Corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
2. **NEVER** open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
3. Delete spam, chain, and other junk email without forwarding, in with Catalyst IT's *Acceptable Use Policy*.
4. Never download files from unknown or suspicious sources.
5. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
6. Always scan a floppy diskette from an unknown source for viruses before using it.
7. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
8. If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

Internet Usage Policy

Overview
Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using or "surfing" the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

Purpose
The purpose of this policy is to define the appropriate uses of the Internet by Catalyst IT employees and affiliates.

Scope
The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

Internet Services Allowed
Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

1. E-mail -- Send/receive E-mail messages to/from the Internet (with or without document attachments).
2. Navigation -- WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.
3. File Transfer Protocol (FTP) -- Send data/files and receive in-bound data/files, as necessary for business purposes.
4. Telnet -- Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the company.

Management reserves the right to add or delete services as business needs change or conditions warrant. All other services will be considered unauthorised access to/from the Internet and will not be allowed.

None Trusted Internet Access
Open WIFI access such as Free public Wi-Fi, provided in coffee shops, rail stations etc. are not be used in any circumstance.

These WIFI locations may not be secured and the laptop and the data maybe exposed to 'Middle Man' attacks where all data (including passwords) are logged without your knowledge.

New Employees

As part of the new employee induction the employee is required to read both this Internet usage Policy and the associated Internet/Intranet Security Policy The user must then sign the statements (located on the last page of each document) that he/she understands and agrees to comply with the policies. Users not complying with these policies could be subject to disciplinary action up to and including termination.
Policy awareness and acknowledgment, by signing the acknowledgment form, is required before access will be granted.

Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

1. Communication between employees and non-employees for business purposes;
2. IT technical support downloading software upgrades and patches;
3. Review of possible vendor web sites for product information;
4. Reference regulatory or technical information.
5. Research

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.
Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

Other activities that are strictly prohibited include, but are not limited to:

1. Accessing company information that is not within the scope of one's work. This includes unauthorised reading of customer account information, unauthorised access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
2. Misusing, disclosing without proper authorisation, or altering customer or personnel information. This includes making unauthorised changes to a personnel file or sharing electronic customer or personnel data with unauthorised personnel.
3. Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
4. Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
5. Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organisation. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

6. Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
7. Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
8. Any form of gambling.

Unless specifically authorised under the provisions, the following activities are also strictly prohibited:

1. Unauthorised downloading of any shareware programs or files for use without authorisation in advance from the IT Department and the user's manager.
2. Any ordering (shopping) of items or services on the Internet.
3. Playing of any games.
4. Forwarding of chain letters.
5. Participation in any on-line contest or promotion.
6. Acceptance of promotional gifts.

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

Email Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

Maintaining Corporate Image

Representation

When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.

Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee's manager and the public relations department and will be placed by an authorised individual.

Creating Web Sites

All individuals and/or business units wishing to establish a WWW home page or site must first develop business, implementation, and maintenance plans. Formal authorisation must be obtained through the IT Department. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted

to the Corporate Communications Directors for initial approval to continue. All company pages are owned by, and are the ultimate responsibility of, the Corporate Communications Directors.

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the IT department.

Policy Compliance

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the IT Team in advance.

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

Software Installation Policy

Overview
Allowing employees to install software on company computing devices opens the organisation up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organisation's network are examples of the problems that can be introduced when employees install software on company equipment.

Purpose
The purpose of this policy is to outline the requirements around installation software on Catalyst IT devices. To minimise the risk of loss of program functionality, the exposure of sensitive information contained within Catalyst IT's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

Scope
This policy applies to all Catalyst IT employees, contractors, vendors and agents with a Catalyst IT-owned mobile devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within Catalyst IT.

Policy
1. Employees may not install software on Catalyst IT's computing devices.
2. Software requests must first be approved by the requester's manager and then be made to the IT department or to the Technical Director via email.
3. The IT Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

Policy Compliance

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the IT team in advance.

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

Web Application Security Policy

Overview
Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities by remediated prior to production deployment.

Purpose
The purpose of this policy is to define web application security assessments within Catalyst IT. Web application assessments are performed to identify potential or realised weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Catalyst IT services available both internally and externally as well as satisfy compliance with any relevant policies in place.

Scope
This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Catalyst IT.

All web application security assessments will be performed by delegated security personnel either employed or contracted by Catalyst IT. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of Catalyst IT is strictly prohibited unless approved by the Technical Director.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

Policy
Web applications are subject to security assessments based on the following criteria:

1. **New or Major Application Release** – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
2. **Third Party or Acquired Web Application** – will be subject to full assessment after which it will be bound to policy requirements.
3. **Point Releases** – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
4. **Patch Releases** – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
5. **Emergency Releases** – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology.

Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

1. **High** – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
2. **Medium** – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
3. **Low** – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

The following security assessment levels shall be established by the IT organisation or other designated organisation that will be performing the assessments.

1. **Full** – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
2. **Quick** – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
3. **Targeted** – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

Precise tools and techniques will be used depending upon what is found in the initial security scanning assessment and the need to determine validity and risk are subject to the discretion of the IT Team.

Related Standards, Policies and Processes

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt.

All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Technical Director.

Please review the following standards for application testing and design:

- OWASP Top Ten Project
- OWASP Testing Guide
- OWASP Risk Rating Methodology

Policy Compliance

Compliance Measurement
The IT team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be approved by the IT team in advance.

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

Database Credentials Coding Policy

Overview
Database authentication credentials are a necessary part of authorising application to connect to databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organisation.

Purpose
This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Catalyst IT's networks or client delivery.

Software applications produced by Catalyst IT may require access to one of the many servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database may be compromised.

Scope
This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the Catalyst IT Network or producing solutions for end Customers. This policy applies to all software (programs, modules, libraries or APIS that will access a Catalyst IT, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitised information.

General
In order to maintain the security of Catalyst IT's databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Specific Requirements
Storage of Database User Names and Passwords

1. Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
2. Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
3. Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
4. Database credentials may not reside in the documents tree of a web server.
5. Pass through authentication (i.e., Oracle OPS authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
6. Passwords or pass phrases used to access a database must adhere to the *Password Policy*.
7. Retrieval of Database User Names and Passwords
8. If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
9. The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
10. For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

Access to Database User Names and Passwords

1. Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
2. Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
3. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Policy Compliance

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT team in advance.

Non-Compliance

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

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Catalyst IT.
Any program code or application that is found to violate this policy must be remediated within a 90 day period.

Bring Your Own Device Policy

Overview
Catalyst IT grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. Catalyst IT reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of Catalyst ITs data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Purpose
All employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use
1. The company defines acceptable business use as activities that directly or indirectly support the business of Catalyst IT.
2. The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
3. Devices may not be used at any time to:
4. Store or transmit illicit materials
5. Store or transmit proprietary information belonging to another company
6. Harass others
7. Engage in outside business activities
8. Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, SharePoint, CRM
9. Catalyst IT has a zero-tolerance policy for texting or emailing while driving and hands-free talking while driving is not permitted.

Devices and Support
1. Smartphones including iPhone, Android, Blackberry and Windows phones are allowed.
2. Tablets including iPad and Android are allowed
3. Connectivity issues are supported by IT; employees should/ contact the device manufacturer or their carrier for operating system or hardware-related issues.
4. Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Reimbursement
1. The company will not reimburse the employee for a percentage of the cost of the device (include the amount of the company's contribution).
2. The company will a) pay the employee an allowance, b) cover the cost of the entire phone/data plan, c) pay half of the phone/data plan, etc.
3. The company will not reimburse the employee for the following charges: roaming, plan overages, etc.

Security
1. In order to prevent unauthorised access, devices must be password protected using the features of the device and a strong password is required to access the company network.
2. Catalyst Recommend that strong passwords are used wherever possible
3. The device must lock itself with a password or PIN if it's idle for five minutes.

4. After five failed login attempts, the device will lock. Contact IT to regain access.
5. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
6. Smartphones and tablets belonging to employees that are for personal use only are allowed to connect to the network after authorisation from IT.
7. Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

Risks/Liabilities/Disclaimers

1. While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
2. The company reserves the right to disconnect devices or disable services without notification.
3. Lost or stolen devices must be reported to the company within 24 hours at the latest. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
4. The employee is expected to use his or her devices to adhere to the company's acceptable use policy as outlined above.
5. The employee is personally liable for all costs associated with his or her device.
6. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
7. Catalyst IT reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Policy Compliance

Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the IT team in advance.

Non-Compliance

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

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Catalyst IT.
Any program code or application that is found to violate this policy must be remediated within a 90 day period.