GLOSSARY

Access
There are two types of access – **Physical** and **Logical**.

1. Physical Access. The process of obtaining use of a computer system, - for example by sitting down at a keyboard, - or being able to enter specific area(s) of the organization where the main computer systems are located.
2. Logical Access. The process of being able to enter, modify, delete, or inspect, records and data held on a computer system by means of providing a User ID and password.

Access Control
A principle of limiting access to computerized information to authorized individuals or information systems (applications, systems, etc.). It refers to the rules and deployment mechanisms that control access to information systems, and physical access to premises.

Access Point (AP):
A hardware device that connects wireless clients to the City network. Usually mounted on ceilings or high walls.

Access Rights
The powers granted to users to create, change, delete, or view data and files within a system.

Account
A mechanism used to control access to information systems and assign access rights (e.g. a User ID). Before resources on systems are utilized, accounts must be created for users or processes.

Accountability
A principle that enables all actions to be traced back to an individual who may be then be held responsible for their actions.

Anti-Virus Program
Software designed to detect, and potentially eliminate, computer viruses, as well as repairing or quarantining files which have already been infected by virus activity.

Appliance
Specialized equipment that is designed for ease of installation and maintenance. Appliances typically have their hardware and software bundled and pre-installed. An appliance is intended to connect into an existing environment and begin working almost immediately, with little configuration. Appliances typically contain vendor-supplied or embedded operating systems and are vendor supported.

Application
A software program or group of software programs used to perform specific business functions for multiple users, or in some cases other software programs.

Application Architecture
The fundamental organization (i.e. architecture) of an information system (i.e. application). Defines process, data, and technology components and their relationships.

Archive
An area of data storage set aside for non-current (old or historical) records in which the information can be retained under a restricted access regime until no longer required by law or organization record retention policies.

Archiving
The process of moving non-current records to the Archives.

Authentication:
A method of proving that the identification (usually a User ID) presented to an information system is valid. This is typically a password. There are three types of authentication:
Type 1. Something only the user knows such as a password, response to a challenge question, etc.
Type 2. Something the user has, such as a SecurID token, smart card, etc.
Type 3. Something the user is (biometrics), such as fingerprints.
Authentication systems can use any single method, a combination of any two methods (two-factor authentication) or use all three methods (three-factor authentication). Note: using two authentication methods of the same type (e.g. using two passwords to authenticate to a computer) is not two-factor authentication.

Authorization:
1) The resources and access rights granted to a user, process, system, etc. after the person/process/etc. is authenticated.
2) The process whereby a person approves a specific event or action.

Availability
The assurance that information remains accessible when required. Availability is a security goal and one of the elements of the Confidentiality, Integrity, and Availability (CIA) classification model. It relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities. If a mission-critical IT system is unavailable to its users, the organization's mission may be affected.

Backup
The process whereby copies of computer files are made in order to allow recreation of the original, should the need arise. A backup is a spare copy of a file, system, or other information resource for use in the event of failure or loss of the original.

Batch
The execution of a series of programs on a computer without human interaction.

Batch User ID

An identification code (User ID) used to perform a batch (a sequence of commands or a group of tasks run in non-interactive background mode) processing.

Business Case

The Business Case forms the foundation for any proposed venture or project. It establishes (in commercial / business terms) the need, justification and proposed alternatives to resolving a business issue or meeting a strategic objective.

Business Continuity Plan (BCP)

A predefined set of actions that provide the ability to assess the impact of an event, activate appropriate actions, recover critical business operations, and restore normal business processes. This is a plan to ensure that the essential business functions of the organization are able to continue (or re-start) in the event of unforeseen circumstances, normally a disaster of some sort. However, BCP is not to be confused with Disaster Recovery Planning, which is focused upon crisis management.

Having dealt with the immediate crisis: securing the health and safety of people and preventing further spread or continuation of the crisis (e.g. a fire), the Disaster Recovery Plan will hand over to those responsible for executing the Business Continuity Plan. The BCP will identify the critical people (roles / functions), information, systems and other infrastructure, e.g. telephones, which are required to enable the business to operate. The BCP will lay out a detailed plan that, if called upon, should be executed to assure minimum additional disruption.

Business Requirements

The needs of the business processes that must be addressed by either a manual or computerized system. It is critical that the business requirements be clearly defined and documented.

Capacity Planning

Capacity Planning is the determination of the overall size, performance and resilience of a computer or system. The detailed components of a Capacity Planning initiative will vary, depending upon the proposed usage of the system, but the following should always be considered:

- The expected storage capacity of the system and the amount of data retrieved, created and stored within a given cycle.
- The number of on line processes and the estimated likely contention.
- The required performance and response required from both the system and the network i.e. the end-to-end performance.
- The level of resilience required and the planned cycle of usage – peaks, troughs and average.
- The impact of security measures e.g. encryption and decryption of all data.

Change Control

An internal control procedure by which only authorized amendments are made to the organization's software, hardware, network access privileges, or business process etc.

Commercial software

Software for which the City receives authorization through receipt of a license for the "right to use" the product from the originating person, organization, or City. In general, the City pays a fee for the license, although this is not always a requirement. Commercial software is protected by copyright. The owner of a copyright for software, usually the developer, has the right to prohibit other people from making copies, except as stated in a license or in copyright law.

Commission
The commissioning of a (computer) system is the point when it is put into live, operational, and active service.

City-owned software
Software written by City employees or by persons under contract to the City whereby the City acquires copyrights to the software. This software must not contain any commercial or third-party software unless permission for use has been granted by the copyright owners of the software.

Computer:
A programmable device that performs mathematical calculations and logical operations, especially one that can process, store and retrieve large amounts of data very quickly. A computer runs an operating system (such as Microsoft Windows), can have peripheral hardware (such as a monitor, mouse, keyboard, printer, etc), and runs application programs (such as word processing applications, web browsers, mobile apps, etc.). This definition includes but is not limited to desktops, laptops, and mobile devices.

Computer Systems:
One or more computers, with associated peripheral hardware, with one or more operating systems, running one or more application programs, designed to provide a service to users. Includes desktops, laptops, and mobile devices.

Computer Virus
Pieces of programming code which have been purposely written to inflict an unexpected result upon a computer system.

Consultant
A user who works directly in the City under a contract between the City and the user, or the user's employer.

Contract Services
A user who works directly in the City under a contract between the City and the user's employer.

Controls
Controls are automatic or manual countermeasures intended to prevent, detect, or correct errors, omissions, accidents, or deliberate acts that could affect the computer's accuracy, integrity, availability, or security. Unless otherwise stated controls are mandatory. Controls meet broad policy objectives. For example, a policy might require that sensitive data be

protected on removable media (Portable media, CD-ROM, etc.). The control would be to encrypt the data on removable media.

Core

Core technology represents the strategic infrastructure direction of the City. All strategic investments should be made according to the core technology standards. Core components are replicated and supported throughout the City.

Core Declining

Core-declining technology represents technology that previously was core, but which does not represent the present strategic direction for City technology investments. It may be broadly deployed and may be required for the processing of critical systems. The expectation is that core-declining technology will gradually be replaced by core technology.

Data

- Computerized information.
- Information processed by an information system and owned by the originator of the information.
- The smallest discrete unit of information organized in a database that needs to be combined with other data and processes in order for it to be understood.

Data does not necessarily represent a record because it may or may not have been created in the conduct of business, and preserved as evidence of a decision or action.

Data Center

A room or building used primarily to house computer equipment, power, and air conditioning supply areas. This equipment is usually located in a special room because of the need for physical security, temperature control, power redundancy, and fire protection.

Data Owner

The person who creates, or initiates the creation or storage of the information, is the initial owner. In an organization, possibly with divisions, departments and sections, the owner becomes the unit itself with the person responsible, being the designated 'custodian' of that data.

Database

A collection of files, tables, forms, reports, etc., held on a computer system that have a predictable relationship with each other for indexing, updating, and retrieval purposes.

Decryption

The process by which encrypted data is restored to its original form in order to be understood/usable by another computer or person.

Desktop

Verbal shorthand for Desktop Personal Computer, normally used to differentiate such a system from a 'Laptop' or portable PC.

Digital Certificate

A digital certificate is the electronic version of an ID card that establishes the user's credentials and can be used to authenticate connections over the Internet or Intranet.

Digital Signature:
A process applied to an electronic communication that verifies the sender's identity and validates that the message was not forged or modified.

Distributed Processing
Spreading the organization's computer processing load between two or more computers, often in geographically separate locations.

Downtime
The amount of time a system is down in a given period. This will include crashes and system problems as well as scheduled maintenance work.

Electronic Data
Data stored on electronic storage media.

Electronic Communications
Computer-facilitated communications including but not limited to: email, instant messaging (IM), and text messaging.

Electronic Mail (Email)
A method of exchanging digital messages from an author to one or more recipients via an electronically transmitted message. This message is stored on and retrieved from an organization's server.

Electronic Storage Media
Storage devices in computers or any removable storage medium which is capable of storing data in an electronic format, such as a computer hard drive, CD, DVD, USB drive, digital memory card, personal digital assistant (PDA), personal media player, cell phone or other similar device.

Emerging technology
Emerging technology represents technology that the City is considering for eventual deployment into core technology or into a peripheral role. Emerging technology can represent a unique new service for the infrastructure or the same service, but with a significantly new product or standard.

Encryption
The process of coding information so that its content is not understandable to anyone who obtains the information. To read the information, an algorithm is required to restore the information to its original form. Information also may be one-way encrypted so that it is not possible to restore the information to its original form. One-way encryption typically is used to protect passwords while they are stored on a computer system.

Enterprise Network

Term meant to encompass all City controlled networks.

End-User
The person who actually uses the hardware or software that has been developed for a specific task.

Event
A situation or set of circumstances that may lead to the loss, prevention or reduced functionality of a business process.

External Email
Email sent, or received from, outside the City Networks.

External Facing
Applications and websites that are accessed by external users (including but not limited to suppliers, dealers, consumers, etc.) and all City web systems (developed internally or externally) that reside on the extranet or Internet.

Firmware
Software or code stored permanently or semi-permanently on a memory chip.

Graphical User Interface Guidelines (GUI)
A type of user interface that allows users to interact with electronic devices with images rather than text commands.

Hard copy
A copy on paper, as opposed to any other storage medium.

Hardware Physical equipment:
Computers, screens, keyboards, mice, printers, scanners, network routers, switches, racking, disk drives, portable drives, etc.

Help Desk
ITSU Staff who are responsible for assisting other staff members in the use of computer systems, resolving problems which may arise, and routing failures or advanced issues to the appropriate IT personnel.

Host
An information system contacted through a network by subordinate computers (PCs, terminals, etc) for processing or information. An endpoint device.

Independent Contractor
User works directly in the City under a contract between the City and the user.

Information Management
The coordinated management of a City's information-based resources, including its information holdings and investments in technology.

Information Systems
Information Systems (also referred to as "systems") – The computer systems and information sources used by an organization to support its day-to-day operations. Examples include applications, infrastructure, tools, appliances and web sites.

Information Systems Owner
The operational activity (stakeholder) whose business process is supported by the information system. The stakeholder is the committee or individual who controls the maintenance and development budget for the information system. If an information system has more than one owner, a primary owner or a steering group with representatives from all owners, should be designated. The owner of the information system may also assess the risk and identify the security and control requirements that must be met to protect the information system.

Infrastructure
Hardware devices and/or software components which provide the underlying foundation or framework that enables and supports applications. Functions that infrastructure provide include, but are not limited to, operating system functions, backup and recovery, communication & messaging, networking, database management, scheduling, user access security, and physical security. Examples of Infrastructure include, but are not limited to: Windows, Linux, Virtual Machines (VMs), SQL, scheduling software, badge reader software, etc.

Infrastructure Control Review (ICR)
A process to ensure that effective controls are designed and implemented for infrastructure, appliances and similar systems.

Integrity
The assurance that information is accurate and has not been improperly modified, either intentionally or unintentionally. Integrity is a security goal and one of the elements of the CIA classification model. It relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations. Integrity is lost if unauthorized changes are made to the data or IT application by either intentional or accidental acts. If the loss of application or data integrity is not corrected, continued use of the contaminated application or corrupted data could result in inaccuracy, fraud, or erroneous decisions.

Internet (also Public Internet)
A publicly accessible Wide Area Network that can be employed for communication between computers. Some features of the Internet include Search Engines, Social Networking, Bulletin Boards, On-Line services, and a variety of other accessible networks.

Intranet
A Local Area Network within an organization, which is designed to look like, and work in the same way as, the Internet. Intranets are essentially private networks, and are not accessible to the public.

Intrusion

The IT equivalent of trespassing. An uninvited and unwelcome entry into a system by an unauthorized source. While Incursions are always seen as Hostile, Intrusions may well be innocent, having occurred in error.

IT Manager

The individual responsible for the technical development, implementation, and/or operational support of a computer system.

ITPM - IT Policy Manual.

The publication that contains IT Policy for the City.

Laptop

A portable computer

Load / System Load

The 'load' on a system refers to the demands placed upon it. The overall load combines many factors and includes:

- Total storage capacity for programs and data
- Number of applications being run concurrently
- Number of concurrent users, peaks, troughs and average
- Number of peripherals: e.g. using a file server as a print server increases demand, as each printed document is 'spooled' to the server's disk before being queued to the printer.

Local Area Network (LAN)

A private communications network owned and operated by the City within one location. This may comprise one or more adjacent buildings, but a local network will normally be connected by fixed cables or short range radio equipment.

Malicious Software (Malware)

Software that causes unauthorized destruction, damage, or unauthorized changes to software, data, or unauthorized use of computer equipment and communication networks.

Media

The physical material which stores computer information. Comes in two basic types - Fixed and Removable and include:

Hard Disk, External Hard Disk, USB Drive, Memory Card, CD, DVD, Floppy Disk, Zip Disk, Magnetic Tape Cartridge, etc.

Need to know

A control principle that ensures that an entity (user, computer processes etc.) is only given sufficient access or authority to complete the entities job function or task.

Non Disclosure Agreement (NDA)

A Non Disclosure Agreement (NDA) is a legally binding document which protects the confidentiality of ideas, designs, plans, concepts or other commercial material. Most often, NDA's are signed by vendors, contractors, consultants and other non-employees who may come into contact with such material.

Official Record
A record with long-term business, legal, or regulatory value.

Operating System

- Software that controls the execution of application programs, resource allocation, scheduling, input/output, and data management
- Computer programs that are primarily or entirely concerned with controlling the computer and its associated hardware, rather than with processing work for users. Computers can operate without application software, but cannot run without an operating system.

Patch
A patch is a software release created to overcome software problems, including glitches and security flaws.

PC
A PC is defined for the purpose of this policy, as a City-assigned personal computer, or workstation.

Phishing
Phishing scams are typically fraudulent email messages appearing to come from legitimate enterprises (e.g., your bank, Internet service provider, the government). These messages usually direct you to a fraudulent web site or otherwise try to get you to divulge private information (e.g., usernames, passwords, account numbers, credit card details, social security numbers, or other account updates). The perpetrators then use this private information to commit identity theft or other crimes.

Policy
Policies are high-level management statements, instructions or business rules that provide guidance to enable individuals to make present and future decisions. Policies are mandatory. Special ITSU management-approval is required when anyone wishes to take a course of action that is not in compliance with policy.

Priority Applications
The sequence of recovery for applications based on their impact to City operations

Private Key
A key used to digitally sign outgoing electronic communication messages/data and decrypt incoming messages/data.

Procedures

Procedures are specific operational steps or manual methods that support a policy or a standard.
For example, a policy could describe the need for back-ups. A standard could define the software to be used to perform back-ups and how to configure this software. A procedure could describe how to use the back-up software, the timing for making back-ups, etc.

Production / Live
When a system is 'in production' or 'live', the system is being used to process active work or transactions, and it is no longer in test/development mode. There must be clear differentiation between systems which are being evaluated, tested, or developed from those which are 'live'.

Project
A plan, including scope, deliverables, work, duration and budget which follows an appropriate Systems Development Methodology.

Publicly Display
To exhibit, hold up, post, or make visible or set out for open view, including, but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public or in a public manner.

Public-domain software
Software available to anyone free of charge. Public-domain software is not protected by copyrights. A license or other obligation is not necessary for its legal use. Generally, support is not available. The software can only be obtained in an "as is" condition.

Remote Site
A secure building located outside the range of environmental hazards that could affect the primary computer center.

Remote Storage
A secured storage location in another building with sufficient distance from the original location to ensure its availability in the event that a disaster occurs in the original location.

Risk Management
The process of assessing the threat, the vulnerabilities, and the value of an asset and applying cost effective controls. The purpose of risk management is to balance the risk of loss, damage, or disclosure of an asset against the costs of controls and to select the mix that provides adequate protection without excessive cost in dollars or in the efficient flow of information to those who require ready access to it. The use of a risk management process provides a rational, cost-effective framework as the underlying basis for security decision making.

Separation of duties
A control principle that reduces or eliminates the risk of accidental or intentional misuse of assets (includes business transactions, information etc.) by ensuring that no single individual or process has total control over an asset.

Server
Typically a powerful, special purpose computer which supplies (serves) a network of less powerful machines such as desktop PCs, with applications, data, messaging, communications, information, etc..

Service Level Agreement (SLA)
A Service Level Agreement (SLA) is a contract between two entities (e.g. the City and a vendor or between service units within the City - Data center and Application Owner) to provide a range of support services, up to an agreed minimum standard.

Shareware
A special category of commercial software that is distributed initially without a license. If, after an evaluation period, the user has found the software to be useful, the user may be expected to pay a fee. City users of shareware must pay fees required by a shareware developer. A purchase notification (purchase order or release against a blanket order including The City terms and conditions for software) must be issued to the developer in exchange for a license to continue to use the product. Use of the software must be approved by ITSU management prior to installation or use on City computer systems.

Sign off
An agreement, as evidenced by the customer's signature, that the system or project, meets the specified requirements.

SME
Subject Matter Expert. A person with knowledge in a specific subject area, who is consulted as an expert in that subject.

Standards
Standards are mandatory. They are the next level below policies and include details such as; implementation steps, systems design concepts, software interface specifications, technologies used, and other specifics. Standards may change considerably more often than policies because the associated manual procedures, organizational structures, business processes, and technologies change so rapidly.

Technology Resources
Technologies and information resources used for City information processing, transfer, storage, and communications. Included in this definition are computing and electronic communications devices and services such as workstation computers, laptops, mobile devices (smart phones, tablets, PDAs), networks, printers, electronic communication systems (e-mail, instant messaging, etc.), telephones, digital media, and Internet services. This definition is not all inclusive but rather reflects examples of City of Ann Arbor equipment, supplies, and services.

Tool
A program used for software development or system maintenance. Any program or utility that helps IT personnel or users develop applications or maintain their systems are tools.

Trojan Horse
A software program or command procedure containing malicious hidden code that, when invoked, performs some unwanted function, such as opening a "back door" to the system through which an attacker can connect.

Two-factor Authentication
There are generally three forms of authentication: something a person knows (such as a password), something a person has (such as a bank card or token device), and something a person is (such as a fingerprint or other measure taken from the human body). Two-factor authentication is a type of strong authentication that requires two of the three forms.

User ID (User Name, ID)
A unique identifier that is associated directly with an individual and remains with the person throughout their employment with the City. When the person transfers to a new job, the authorities assigned to the User ID must be changed to reflect access requirements of the new job. Personal User IDs are to be used when accountability for access or changes to data is required.

Users
People who are authorized to use City of Ann Arbor Computer Systems. It includes City employees, volunteers, authorized contractors, and non-regular workforce on assignment to the City.

Virus
A malicious self-replicating program that repeatedly attaches itself to application programs or to any other executable system component to gain control during some phase of execution and to continue the replication process.

Visitor
Individual who is not a regular user of the system and has no registered/recognized User ID or password.

Web Site
A Web site is a collection of Web pages that are generally accessible over the Internet or Intranet using the HTTP protocol. The pages of a website are accessed from a common root URL (the home page) and may reside on the same physical server or multiple servers.

- **Static Web Site**
  A web site containing web pages that supply the web browser with information that is pre-formatted and written into the HTML code. Data on a static web page cannot change without changing the source code of the page itself.
- **Dynamic Web Site**
  A web site containing web pages that retrieve content from sources outside the HTML code (typically a database), either via choices from the user or page defaults.

Wide Area Network
A communications network that extends beyond the City's immediate premises.

Wi-Fi Protected Access (WPA/WPA2):
A security protocol that encrypts data over the WLAN.

Wired Equivalent Privacy (WEP):
A security protocol that encrypts data over the WLAN. Insecure and deprecated. Wi-Fi Protected Access (WPA/WPA2) should now be used.

Wireless Infrastructure
All components (access points, wireless bridges, wireless repeaters, authentication servers, etc) that create a wireless network whether standalone wireless or providing connectivity to the wired infrastructure.

Worm
A malicious program that uses network connections to spread from system to system automatically. Like a virus, a worm has the ability to infect other systems as well as other programs. A worm will typically expand continuously until it utilizes all available system resources.