Catalyst Information Security Program Brief

Information Security Program

Information is one of Catalyst's most valuable assets. In order to maintain and establish trust between Catalyst and its Supporters, the protection of information is critical. While Catalyst encourages flexibility in how and where work is done, the security of its data is a core element of its philosophy. The Information Security Program, and its supporting policies and standards, have been formulated in order to provide staff with a clear understanding of their responsibility toward protecting informational assets

1. **Acceptable Use**

   This Policy outlines the use of company technology resources and ensures employees understand what is considered acceptable use. Incidental personal activities are permitted, as long as the privilege is not abused. The policy applies to all company-owned information technology tools and information technology services, including e-mail, voice mails, and the Internet, regardless of location. It also applies to third parties performing services on Catalyst's behalf.

   Catalyst maintains an inventory of technologies used in the Catalyst Network. IT equipment must be adequately secured when taken off-site. Departing employees must return all Catalyst Information Resources to IT in good working condition. The return of Catalyst Property/Information Resources includes, but is not limited to, all confidential information.

2. **Anti-Malware**

   Catalyst must stop malicious software while effectively and efficiently achieving its business objectives with anti-malware technologies. The goal is to ensure that activity stemming from malicious software (Viruses, Trojans, Worms, Spyware) is prevented or mitigated. Removable media such as USB and DVD-ROM will be disabled and generally not permitted to be connected to Catalyst laptops.

3. **Bring Your Own Device**

   The policy applies to all mobile and handheld devices, whether owned by Catalyst or by employees. Devices must use a currently-supported Operating System: Android, iOS/iPad OS and Windows 10. Users must contact the Device manufacturer or mobile carrier for operating system, hardware or data connectivity issues. The policy does not apply to Catalyst-owned, IT-managed laptops. The employee is personally liable for all costs associated with their Device

   Catalyst will respect the privacy of the employee's personal data. Catalyst assumes no liability for the loss of personal data. Catalyst will not use MDM software to access a user's personal accounts, applications, contacts, email, text or other messages, photos and social networking activity. However, there is no expectation of privacy with respect to content created or transmitted in connection with Catalyst business.

4. **Cloud Vendor Management**

   Cloud computing is a method of delivering IT services where the customer pays to use, rather than own, the resources. These services are typically provided by third parties via the Internet. All Cloud Services must 1. Be fit for the purpose they are designed to support; 2. Comply with all relevant legislation and regulations (i.e. GDPR, PCI, SHIELD); 3. Comply with all existing Catalyst Policies and Standards; 4. Respect the intellectual property rights of others and not breach

copyright; 5. Comply with the relevant professional ethics and with Catalyst's ethical principles; and 6. Not relinquish any Catalyst data ownership rights.

5. Data Classification

The Data Classification Standard is intended to protect confidentiality, integrity and availability of Catalyst data. All Catalyst data must be assigned an appropriate sensitivity classification ("public," "internal" or "restricted"). Internal is the default classification.

All information possessed by or used by an organizational unit within Catalyst must have a designated Information Steward. Information Technology department does not 'own' Catalyst data. Information Stewards are responsible to store all data in locations that support retention and disposition standards. Information Stewards must be notified if sensitive information is lost, disclosed or suspected of being lost.

6. Employee Privacy (for non-US employees)

Catalyst collects, uses and discloses personal information about each employee. Data includes name, title, addresses, telephone numbers, and personal email addresses. Data is shared with third parties such as references, payroll providers, insurance companies, financial institutions, government agencies and medical professionals. Catalyst retains personal information as long as it is required to fulfill the purpose for which it was collected. Employees must keep personal information in their employee file current and accurate.

7. Data Subject Rights Request Procedure (Deletion Request Procedure)

Under GDPR and other data privacy laws, data subjects have the right, under certain circumstances, to have Catalyst provide, correct, or erase their personal data. This Procedure provides the internal steps to be taken by Catalyst in responding to any data subject rights requests under GDPR. The Chief Privacy Officer will determine whether Catalyst is required to delete the requested personal data.

8. Incident Response

This Plan is designed to assist Catalyst and any applicable third parties in quickly and efficiently responding to and recovering from different levels of security incidents. Security Incidents must be reported immediately upon discovery. The Incident Response Team ("IRT") is responsible for managing Incidents involving loss or unauthorized access of personal data and personal information. Catalyst's CFAO and Communications and Legal Departments will determine how to communicate the breach. Catalyst will hold a "lessons learned" meeting after every major security incident.

9. Information Governance

This Policy is intended to establish the principles of information governance for the protection, management and disposition of Catalyst information. Information may only be accessed by those with a legitimate business need to view, edit or use the data. All individuals with access to Catalyst information must identify, classify, protect, retain and dispose of Catalyst information in accordance with fundamental information governance principles.

10. Internet Use Monitoring and Filtering

This Standard is intended to define standards for systems that monitor and limit web use from any host within Catalyst's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner. The following categories of websites will be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Gambling
- Hacking
- Illegal Drugs
- Peer-to-Peer File Sharing
- SPAM, Phishing and Fraud
- Spyware and malware
- Violence, Intolerance and Hate

If a site is mis-categorized, employees may request the site be unblocked by submitting a ticket to the IT Help Desk. If an employee needs access to an appropriately categorized, blocked, site, the employee's manager will submit a request to Human Resources. HR will present all approved exception requests to the IT Department in writing or by email.

11. Log Monitoring

Logs from critical systems, applications and services can provide key information and potential indicators of compromise of security. The retention and review of logs are critical from a forensics standpoint. This Standard applies to core networking infrastructure such as firewalls and routers in addition to critical servers on the Catalyst network.

Logs shall identify or contain at least the following elements: Type of action, type of data element, date, time, and whether action was allowed or denied by access-control mechanisms. An employee who violates this Standard may be subject to disciplinary action, up to and including termination of employment.

12. Network Security

This Standard defines the precautions designed to safeguard Catalyst's systems, networks and Catalyst data. When applied, this Standard will reduce the risk associated with the misconfiguration and misuse of network systems and services by specifying the control that shall be present within the network systems

13. Password

The purpose of this Standard is to establish a standard for creation and protection of strong passwords. A poorly chosen password may result in unauthorized access and/or exploitation of Catalyst's resources. All users, including contractors and vendors with access to Catalyst systems, are responsible for taking the appropriate steps to select and secure their passwords.

14. Patch and Vulnerability Management

This Standard describes the patch and vulnerability management requirements for maintaining effective protection against internal and external attacks to protect applications and systems managed by Catalyst.

15. **Physical Security**

This Policy is intended to establish standards for securing access to Catalyst offices, data centers, network closets and Information Technology (IT) facilities. Effective implementation of this Policy will minimize unauthorized access to these locations and provide more effective auditing of physical access controls. All facilities must be physically protected in proportion to the criticality or importance of their function. The Policy applies to all Catalyst owned or operated facilities.

16. Record Retention and Disposition

The purpose of this Standard is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed by Catalyst or are of no value are discarded at the proper time.

A Record Retention Schedule is approved as the retention and disposal schedule for Catalyst. In the absence of a schedule, a minimum retention of 180 days is required. The Chief Privacy Officer (Administrator) is the officer in charge of the administration of this Standard and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed.

17. Remote Access

This Standard defines requirements for connecting to Catalyst's network from any location other than a Catalyst facility.

18. Reporting of Information Security Incidents and Violations

The Standard is intended to provide direction for user reporting of Information Security Incidents.

19. **Security Awareness Training**

This policy is intended to ensure that security awareness training is conducted for all employees with the goal of better protecting Catalyst’s confidentiality, integrity, and availability of its information resources and data. The Information Technology and Human Resources Department will define and implement an information security awareness training program to increase Users’ awareness of their security responsibilities. Annually, a skills gap analysis will be performed to understand the skills and behaviors employees are not adhering to, and use this information to build a baseline education roadmap. Training will be delivered to address the skills gap identified to positively impact the employee’s security behavior.

20. **Segregation of Duties**

This Standard defines the types of activities which should be separated in order to achieve the objective of properly segregating conflicting duties. Segregation of duties has two primary objectives. The first is the prevention of conflict of interest (real or apparent), wrongful acts, fraud,

abuse and errors. The second is the detection of control failures that include security breaches, information theft and circumvention of security controls. Organizational roles should be structured such that no one Resource (as defined below) is in a position to initiate, approve, and review the same action, transaction, event or process. Management must rate the risk of non-adherence and mitigate the risk with compensating controls.

21. **Software Management**

Allowing employees to install software on Catalyst-owned computing devices exposes the organization to unnecessary risk. Installing unauthorized software can introduce conflicting file versions or DLLs which prevent programs from running, malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can compromise the organization's network. This Standard will minimize the risk of loss of program functionality, the exposure of sensitive information from Catalyst's computing network, the risk of introducing malware and the legal exposure of violating vendor contracts and copyright laws.

22. **User Access Management**

Access to Catalyst systems must be restricted to only authorized users or processes, based on a need-to-know basis and with the least amount of access privilege granted as needed. Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job-related duties. This Standard is intended to describe how accounts and privileges should be used, approved, granted, audited and deprovisioned.