Information Security Policy

April 2016

Table of Contents

PURPOSE AND SCOPE 5

I. CONFIDENTIAL INFORMATION 5
II. SCOPE 6

ORGANIZATION OF INFORMATION SECURITY 6

I. RESPONSIBILITY FOR INFORMATION SECURITY 6
II. COMMUNICATIONS REGARDING INFORMATION SECURITY 7

RISK ASSESSMENT AND TREATMENT 7

I. ASSESSING SECURITY RISKS 7
II. RESPONDING TO IDENTIFIED SECURITY RISKS 7

INFORMATION ASSET MANAGEMENT 8

I. INVENTORY OF INFORMATION SYSTEMS 8
II. CLASSIFICATION OF CONFIDENTIAL INFORMATION 8
III. ACCEPTABLE USE OF INFORMATION ASSETS 8

HUMAN RESOURCES SECURITY 8

I. PRIOR TO EMPLOYMENT 8
II. DURING EMPLOYMENT 9
III. TERMINATION OR CHANGE OF EMPLOYMENT 9

PHYSICAL AND ENVIRONMENTAL SECURITY 9

I. SECURE AREAS 9
II. EQUIPMENT SECURITY 10

THIRD PARTY SERVICE DELIVERY MANAGEMENT 10

I. VETTING 10
II. WRITTEN CONTRACT 11
III. RESPONSIBILITIES EXPLAINED 11
IV. MONITORING PROGRAM 11
V. RETURN OR DESTROY 11
VI. IMPROPER PROCESSING 11

COMMUNICATIONS AND OPERATIONS MANAGEMENT 12

I. System planning and acceptance 12
II. Protection against malicious code 12
III. Backup 12
IV. Network security management 12
V. Control of information media 12
VI. Exchange of information 13
VII. Monitoring 13

ACCESS CONTROL 13

I. External access to Information Assets 13
II. User access management 13
III. User responsibilities 14
IV. Network Access Control 14
V. Operating system Access Control 15
VI. Application Access Control 15

INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 16

I. Information processing 16
II. Cryptographic controls 16

BUSINESS CONTINUITY MANAGEMENT 16

I. Information Security aspects of business continuity management 16
II. Scope 16
III. Integration with general business continuity controls 17
IV. Backups 17

COMPLIANCE 17

I. Legal compliance 17
II. Technical and policy compliance audit 17

ADJUSTMENT OF THIS POLICY 17

I. Periodic re-evaluations 17
II. Other re-evaluations 18
III. Modification 18

PURPOSE AND SCOPE

i. Confidential Information

YourCause, LLC ("**YourCause**" or "**Company**") regularly receives, stores, handles, and generates confidential information about our clients, our employees, and our own business. For purposes of this Information Security Policy, Confidential Information is defined as: (i) information pertaining to or received from an existing or prospective YourCause client, including without limitation any information related to an existing or prospective representation ("**Client Information**"); (ii) information that identifies or can be used to identify individuals who are or were managers, directors, employees of, or applicants for employment by, YourCause, or their dependents or beneficiaries ("**Human Resources Information**"); (iii) information relating to YourCause's or its clients' planned or existing information technology systems and systems architecture, including computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods ("**Technical Information**"); or (iv) business information relating to YourCause including information about its services, profits, organizational structure, business initiatives and other financial information ("**Business Information**"), including, without limitation:

- Information that describes YourCause's managers, stakeholders, partners, service providers or other employees;
- Information that describes YourCause's services, and how such services are administered and managed;
- Information that describes YourCause business strategies, tax interpretations, tax positions and treatment of any item;
- Confidential information of third parties with which YourCause conducts business;
- Any information a reasonable person familiar with YourCause's business and with the legal profession in general would consider

confidential or proprietary, the maintenance of which would be important to YourCause, its clients, its employees; and
- Any other information designated in writing as confidential by YourCause.

ii. Scope

This Policy establishes procedures and rules for protecting YourCause's Information Assets, including both Confidential Information and Information Systems, in accordance with YourCause's legal and ethical obligations and business objectives. It incorporates by reference other policies for managing specific Information Assets, and it includes information from third party vendors servicing YourCause.

ORGANIZATION OF INFORMATION SECURITY

i. Responsibility for Information Security

Management at YourCause is ultimately responsible for Information Security. To facilitate development and implementation of robust Information Security, YourCause's Management Team shall rely on the formally designated members of the Information Security Council as the Information Security Officers. The Management Team or Information Security Council may additionally create or designate working groups, task forces, or committees as needed to implement this Policy. The Information Security Council shall be empowered by the Management Team to develop and implement, directly or indirectly, Information Security controls and policies, including and in accordance with this Policy.

ii. Communications regarding Information Security

Management shall establish procedures to manage communications regarding Confidential Information and Information Security with law enforcement, regulatory officials, clients, and others.

Risk Assessment and Treatment

i. Assessing security risks

YourCause shall conduct periodic risk assessments to identify, quantify, and prioritize information security risks against criteria for risk acceptance that reflect the YourCause's legal and ethical obligations and business objectives in light of the sensitivity of the Confidential Information in question. The schedule of risk assessments shall include, but not be limited to:

- Quarterly application and network vulnerability scans
- Annual automated and manual penetration testing
- Periodic review of personnel files
- Periodic website and internal IT stress tests, utilization, licensures, patches, upgrades, etc.
- Periodic review and updating of the YourCause privacy policy

ii. Responding to identified security risks

For each of the risks identified, YourCause shall select and implement controls as necessary and appropriate to meet the requirements identified through Risk Assessment.

Information Asset Management

i. Inventory of Information Systems

YourCause shall maintain and regularly update the company-wide inventory of important Information Assets for property, plant, and equipment and more frequently as necessary for this and all other Information Assets.

ii. Classification of Confidential Information

YourCause shall develop and regularly update a data classification policy for both Public and Confidential Information that reflects applicable legal and ethical requirements and the nature and sensitivity of the public or confidential information.

iii. Acceptable use of Information Assets

YourCause shall develop, implement, and regularly update rules for the acceptable use of the Company's Information Assets.

Human Resources Security

i. Prior to employment

Prospective employees shall be made aware of their obligations with respect to Information Security at the time of, and as a term and condition of, employment.

Background checks: YourCause shall screen candidates for employment who will have routine access to Confidential Information. Background verification checks will be conducted on all candidates for employment who will in some way be responsible for the receipt or disbursement of funds. These background checks shall be carried out in accordance with applicable legal and ethical requirements.

Employee agreements: YourCause will require all employees to sign an agreement confirming their understanding of and commitment to their security roles and responsibilities, regardless of the nature of the data to which they might have routine access.

ii. During employment

YourCause shall maintain employee awareness about Information Security procedures and the protection of Confidential Information.

Education and training: Employees shall receive appropriate awareness training and regular updates on organizational policies and procedures, as relevant for their job function. Security responsibilities shall be explicitly covered in orientation sessions with new employees.

Disciplinary procedure: Any employee who deliberately processes or attempts to process Confidential Information without authorization or in a manner that violates security procedures shall be subject to appropriate disciplinary action, up to and including termination of employment. Any employee reported to be or found in the course of commission of a crime shall be reported to law enforcement authorities.

iii. Termination or change of employment

YourCause shall manage employee separation from the Company so as to ensure the return or other disposition of all Confidential Information, information processing equipment, or other YourCause property. Relevant managers will be responsible for removing or modifying access rights upon an employee's separation or change of responsibilities.

PHYSICAL AND ENVIRONMENTAL SECURITY

i. Secure areas

YourCause shall protect Information Assets by creating defined security permissions and entry controls designed to protect against unauthorized

access, alteration, and misuse, including from natural or man-made disasters.

ii. Equipment security

YourCause shall protect equipment, including that used off-site or remotely, from unauthorized access and other physical and environmental threats.

Equipment disposal or re-use: Confidential Information or other Company property shall be removed or securely overwritten prior to disposal or re-use of equipment.

Workstations: Employees and on-site Service Providers shall be required to: (1) log back into their computers with a user name and password when they leave them for an extended period of time due to an automatic lockout feature on every computer; and (2) secure their workstations during and at the end of each workday by storing confidential information in their appropriate and designated secure cabinets.

Manufacturers' specifications: Manufacturers' specifications for temperature, humidity, and electrical and power requirements shall be observed with respect to all equipment used to Process Confidential Information.

THIRD PARTY SERVICE DELIVERY MANAGEMENT

Products and/or services shall be procured from Service Providers under terms and conditions designed to preserve the integrity and security of Information Assets.

i. Vetting

YourCause shall screen prospective Service Providers, who shall be required to conduct background verification checks on employees likely to have access to sensitive Information Assets. Furthermore, YourCause shall, no less than once a year, assess Service Providers Information

Security and Risk Management policies and procedures via an Information Security and Risk Assessment Questionnaire.

ii. Written contract

YourCause shall require Service Providers to agree in writing to safeguard Information Assets in accordance with standards at least as stringent as those embodied in this Policy before such Service Providers are permitted to access Confidential Information.

iii. Responsibilities explained

Security responsibilities shall be explicitly explained to any Service Provider working on-site or having remote access to Information Assets, and any such Service Provider shall be required to acknowledge in writing its receipt, understanding of, and willingness to accept such security responsibilities.

iv. Monitoring program

Any access to Information Assets by Service Providers shall be authorized and appropriately limited. Service Provider's access rights shall be reviewed on a regular basis and commensurate with the sensitivity of the Confidential Information accessible by the relevant Service Provider.

v. Return or destroy

At the conclusion of contracted Service Provider's assigned tasks, YourCause shall require the Service Provider to return to the Company or destroy any and all Confidential Information under its control.

vi. Improper processing

Any Service Provider who deliberately processes or attempts to process Confidential Information without authorization or in a manner that violates security procedures shall be subject to contract termination and

other appropriate legal actions. Any Service Provider found to be our reported to be in the course of commission of a crime shall be reported to law enforcement authorities.

Communications and Operations Management

i. System planning and acceptance

YourCause shall regularly update projections of future capacity requirements to reduce the risk of system overload. The operational requirements of new systems shall be established, documented, and tested prior to their acceptance and use.

ii. Protection against malicious code

Those with access to Information Assets shall be made aware of the dangers of malicious code. YourCause shall implement and regularly update controls to prevent the introduction of, detect the presence of, and remove malicious code.

iii. Backup

YourCause shall secure adequate back-up facilities, including off-site facilities, and implement policies designed to ensure that essential Information Assets can be recovered following a disaster or media failure.

iv. Network security management

YourCause shall implement controls designed to ensure the security of information in networks, and the protection of connected services from unauthorized access.

v. Control of information media

Appropriate operating procedures shall be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification,

removal, and destruction. When no longer required, media shall be disposed in a secure and safe manner.

vi. Exchange of information

Formal exchange policies, procedures, and controls, consistent with YourCause's ethical and legal obligations and business objectives, shall be in place to protect Confidential Information during transmission or exchange with clients, Service Providers, and other third parties.

vii. Monitoring

Systems shall be monitored and Information Security events shall be recorded. Operator logs and fault logging shall be used, where appropriate, to ensure information system problems or improper processing are identified.

Access Control

i. External access to Information Assets

YourCause shall establish and regularly update procedures to manage internal and third party access to the Company's Information Assets. Such procedures will include a Risk Assessment to determine security implications and Control requirements, which shall be defined in a written agreement with any party permitted to access the YourCause's Information Assets.

ii. User access management

Access Control policies and procedures shall be designed to cover all stages in the life-cycle of user access to Confidential Information, from the initial registration of new users to the final de-registration of users who no longer require access to YourCause Information Assets.

Privilege management: Access to multi-user systems containing Confidential Information shall be allocated on a need-to-use basis reflecting both YourCause's legal and ethical obligations, as well as the sensitivity of the information to be protected. Access and usage logs shall be created where appropriate and practicable.

iii. User responsibilities

Users shall be made aware of and be obliged to fulfill their responsibilities for maintaining effective Access Controls.

Passwords: Users shall be required to follow good security procedures in the selection and use of passwords. Each user with access to Confidential Information shall have a secret password, known only to that user, which shall: (1) follow the Information Security Council password requirements guidelines; (2) be changed regularly; (3) not be reused for four consecutive quarters; (4) not be stored in login scripts or other computer programs; and (5) be deactivated immediately if reported lost or compromised.

Unattended equipment or media: Users shall be required to terminate user sessions and/or lock equipment and secure information media (including screens, papers, disks, etc.) before leaving equipment unattended and at the end of each workday.

iv. Network Access Control

Access to both internal and external network services shall be controlled to avoid compromise of the security of the network. Controls shall include: (1) limiting user access to those network services necessary for the user's responsibilities; (2) authentication of remote users; (3) control of access to diagnostic and configuration ports; (4) segregation of user access by domain; and (5) institution of security safeguards and usage policies specifically for remote networking.

v. Operating system Access Control

Appropriate security controls shall be used to restrict access to operating systems. As appropriate and practicable, such controls shall provide functionality capable of: (1) authenticating users, in accordance with a defined Access Control policy; (2) recording successful and failed system authentication attempts; (3) recording the use of special system privileges; (4) issuing alarms when system security policies are breached; (5) providing appropriate means for authentication; and (6), restricting the connection time of users.

UserIDs: Each user with access to operating systems shall have a unique identification code ("UserID"), and must immediately report lost or compromised UserIDs. UserIDs shall automatically be deactivated and related files archived if lost or compromised.

Passwords: Passwords shall be required to access operating systems.

vi. Application Access Control

Technology safeguards shall be used to restrict access to and within application systems, and logical access to application software and information shall be restricted. As appropriate, application systems shall: (1) control access to information and application system functions, in accordance with a defined Access Control policy; (2) provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls; (3) not compromise other systems with which information resources are shared.

Information Systems Acquisition, Development and Maintenance

i. Information processing

Appropriate controls, including validation of input data, internal processing, and output data, shall be designed into applications based on requirements established through Risk Assessment.

ii. Cryptographic controls

YourCause shall create and implement a policy on the use of cryptographic controls in Information Systems used to communicate with external parties.

Business Continuity Management

i. Information Security aspects of business continuity management

YourCause shall implement and regularly test and update a business continuity management process designed to minimize the impact on the organization and recover from loss of Information Assets, whether resulting from natural disasters, accidents, equipment failures, deliberate actions, or other causes.

ii. Scope

This process shall include controls designed to identify and reduce risks, prevent incidents, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

iii. Integration with general business continuity controls

This process shall identify the critical business processes and integrate the Information Security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

iv. Backups

This process shall require regular backup of Confidential Information and other sensitive, valuable or critical Information Assets.

COMPLIANCE

i. Legal compliance

YourCause shall document and update the Company's ethical, legal, and contractual obligations with respect to Information Security.

ii. Technical and policy compliance audit

YourCause shall regularly review information systems for compliance with applicable security policies, implementation standards, and documented security controls. The review shall include compliance with internal standards, including this policy, and external standards, such as engineering and security standards promulgated by reputable independent organizations including but not limited to US-CERT, NIST and OWASP.

ADJUSTMENT OF THIS POLICY

i. Periodic re-evaluations

YourCause shall re-evaluate this policy on a periodic basis (at least once annually), taking into account changes in legal, ethical, or contractual

obligations, changes in applicable technical standards and industry practice, and technology or other developments having a material impact on Information Security.

ii. Other re-evaluations

YourCause shall re-evaluate this policy any time its effectiveness is called into question by testing and monitoring, system failures, a material change in business operations, or technology or other developments having a material impact on Information Asset.

iii. Modification

Following such periodic or other re-evaluation, the Information Security Council shall report the findings of any periodic or other re-evaluation to the Executive Team, which shall modify, supplement, or amend this policy as appropriate.

Confirmation of Receipt and Agreement

I have received, read, understood and I am in agreement with the YourCause, LLC Information Security Policy updated on the 1st day of April 2016.

Date Recipient's Signature

Date Manager's Signature