Uplevel
Information Security Policy
Effective Date: 1/01/2021
Version 9.0 Responsible Party: Albert Strong

Table of Contents

Introduction

This policy defines the technical controls and security configurations, end users and system administrators which are required to implement to ensure the integrity and availability of the data environment at Uplevel

It serves as a central policy document with which all employees and contractors must be familiar and defines Uplevel actions and prohibitions that all users must follow. The policy provides the managers within Uplevel with policies and guidelines concerning the acceptable use of Uplevel network/cloud infrastructures, databases, external media, encryption and any other methods used to convey knowledge and ideas across all hardware, software, cloud based, and data transmission mechanisms. All Uplevel employees and contractors must adhere to this policy.

Uplevel recognizes that Information Technology (IT) systems and data are valuable assets which are essential in supporting Uplevel' strategic objectives. Uplevel recognizes its obligations to protect information from internal and external threats and recognizes that effective information security management is critical to ensure the successful enablement of IT and delivery of business functions and services. Uplevel is committed to preserving the confidentiality, integrity, and availability of all physical and electronic assets.

Information security management is an ongoing cycle of activity aimed at continuous improvement in response to emerging and changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorized access, disclosure, modification or destruction and is vital for the protection of information and Uplevel reputation.

Scope

This policy document defines common security requirements for all Uplevel personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of Uplevel in cases where Uplevel has a legal, contractual, or fiduciary duty to protect said resources while in Uplevel custody. In the event of a conflict, the more restrictive measures apply.

References in this document to ‘data’, ‘information’, ‘accounts’, ‘communications’, ‘messages’ and ‘files’ include, but are not limited to, confidential information, customer data, sensitive information, personally identifiable information (PII), protected health information (PHI), and electronically protected health information (ePHI) if applicable.

This policy applies to:

- Systems belonging to, or under the control of, Uplevel;
- Information stored, or in use, on Uplevel systems;
- Information in transit across Uplevel voice or data networks;
- Control of information leaving Uplevel;
- Information access resources;
- All parties who have access to, or use of systems and information belonging to, or under the control of, Uplevel including:
    - Uplevel employees
    - Contractors
    - Temporary staff
    - Interns
    - Partner organizations
    - Volunteers
    - Any other party utilizing Uplevel resources

Application of this policy applies throughout the information lifecycle from acquisition / creation, through to utilization, storage and disposal.

Purpose

Uplevel is committed to the development and maintenance of an Information Security Management process and has developed this Security Policy to:

- Provide direction and support for security in accordance with business requirements, regulations, and legal requirements.
- State the responsibilities of staff, partners, contractors and any other individual or organization having access to Uplevel systems.
- State management intent to support the goals and principles of security in line with business strategy and objectives.
- Provide a framework by which the confidentiality, integrity and availability of resources can be maintained.
- Optimize the management of risks, by preventing and minimizing the impact of security incidents.

- Ensure that all breaches of security are reported, investigated and appropriate action taken where required.
- Ensure that supporting security policies and procedures are regularly reviewed to ensure continued good practices and protection against new threats.
- Ensure information security requirements are regularly communicated to all relevant parties.

System Users

It is the responsibility of any individual or organization having access to Uplevel systems and information to comply with the Uplevel Information Security Policy, associated guidelines and procedures and to take adequate steps to safeguard the security of the systems and information to which they have access.

Implementation and adherence to this policy is the responsibility of all Uplevel employees, partner agencies, contractors and vendors working for Uplevel. It is important that every employee takes seriously, the use, protection and integrity of their own password/s or any other system passwords which they may be privy to from time to time and to encourage, guide and inform staff wherever possible for those who are responsible for the supervision of others.

Organizational Structure

Board of Directors

The level of oversight provided by the Board of Directors is described in the Board Charter. The Board of Directors has an important role in establishing the strategic direction of the organization. The Board of Directors independent from management. Senior Management has responsibility for day to day operations of the organization.

Senior Management

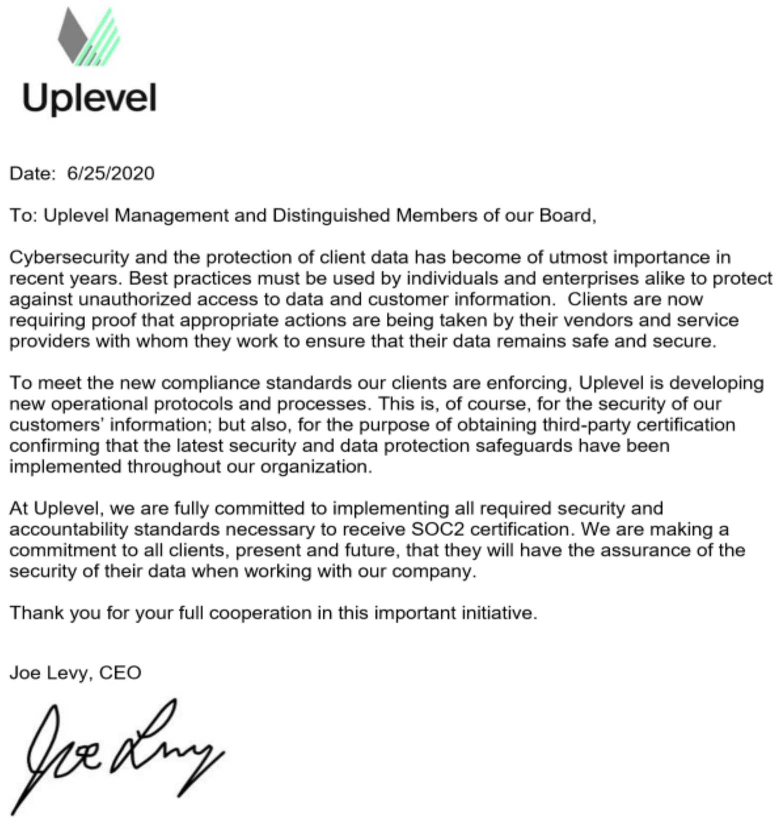
Senior management is responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Uplevel managers are aware they have a responsibility to ensure that staff holds sufficient, relevant knowledge concerning the security of information and systems.

Support for 3rd Party Assessments and Policy of Communication to Board

Uplevel is committed to best practices in the areas of cybersecurity, business process, and financial integrity.

Senior Management by policy is responsible for seeking 3rd Party Assessments as appropriate and timely. Any such assessment will be promptly communicated to the Board.

Letter from CEO Re: Importance of Security



Uplevel

Date: 6/25/2020

To: Uplevel Management and Distinguished Members of our Board,

Cybersecurity and the protection of client data has become of utmost importance in recent years. Best practices must be used by individuals and enterprises alike to protect against unauthorized access to data and customer information. Clients are now requiring proof that appropriate actions are being taken by their vendors and service providers with whom they work to ensure that their data remains safe and secure.

To meet the new compliance standards our clients are enforcing, Uplevel is developing new operational protocols and processes. This is, of course, for the security of our customers' information; but also, for the purpose of obtaining third-party certification confirming that the latest security and data protection safeguards have been implemented throughout our organization.

At Uplevel, we are fully committed to implementing all required security and accountability standards necessary to receive SOC2 certification. We are making a commitment to all clients, present and future, that they will have the assurance of the security of their data when working with our company.

Thank you for your full cooperation in this important initiative.

Joe Levy, CEO

Joe Levy

Key Security Controls	Responsible Party
□ There is a Board Charter	Joe Levy
□ The Board of Directors provides management oversight	Joe Levy
□ The Board of Directors is independent of management and is objective in decision making	Joe Levy
□ Senior Management is responsible for the day to day operations of the company	Joe Levy
□ Senior management is responsible for ensuring that all staff and managers are aware of security policies and that they are observed	Joe Levy
□ Letter from CEO demonstrating commitment to information security	Joe Levy

Key Roles and Descriptions

Uplevel maintains up to date bios of senior executives, an organization chart, and job descriptions for all key roles. This documentation is updated annually.

Uplevel provides a defined chain of command within the company, and to ensure that every employee has a clear area of responsibility such that no critical task can "fall through the cracks." Further, Uplevel ensures that the individuals assigned a specific task are aware of that assignment, are qualified to complete that task, are appropriately monitored for their performance, and are held accountable for their results.

Security Officer

Uplevel has established a Chief Information Security Officer (CISO), who is also the Privacy Officer. This Security Officer will oversee all ongoing activities related to the development, implementation, and maintenance of Uplevel privacy and security policies in accordance with applicable federal and state laws. The current Chief Information Security Officer for Uplevel is: Albert Strong.

Security Review Team

Uplevel has established a Security Board (SRB) made up of key personnel whose responsibility it is to identify areas of concern within Uplevel and act as the first line of defense in enhancing the appropriate security posture.

Members of the Security Review Board are appointed by the Security Officer. The current members of the SRB are:

- Joe Levy
- Nimrod Vered
- Dave Matthews.

The SRB will meet at least Quarterly to discuss security issues and to review concerns that arose since the last meeting. The SRT will identify areas that should be addressed during annual training and review/update security policies, as necessary.

The SRB will address security issues as they arise and recommend and approve immediate security actions to be undertaken.

Separation of Duties Policy

Scope

These requirements apply to PRIVO’s Information Systems

Definition

Separation of Duties (SoD, sometimes referred to as "Segregation of Duties") is an attempt to ensure that no single individual has the capability of executing a particular task/set of tasks. This is a concept familiar to those in the financial industry, where for example, staff who enter accounts payable invoices into the system are not allowed to then approve them as well.

In the context of implementing SoD at PRIVO, this requirement is to ensure accountability as well as limit the ability of individuals to negatively impact the Confidentiality, Integrity, or Availability of the particular Information System.

Policy

System Owners must identify the relevant IT roles for their Information Systems. Once identified, SoD must be implemented such that critical/operational IT functions are separated into distinct jobs to prevent a single person from harming a development or operational system or the services it provides, whether by an accidental act, omission, or intentional act.

The roles identified (and implementation of SoD) must be listed in the particular Information System's security plan.

Enforcement

Management responsible for the secure operation of the Information System is held accountable for implementing SoD to mitigate the risks.

See Also Separation of Duties in Change Management Section

Key Security Controls	Responsible Party
❑ Maintain up-to-date bios for all key executives	Albert Strong
❑ Maintain an up-to-date org chart for all key executives	Albert Strong
❑ An Senior Officer is named as Chief Information Security Officer	Joe Levy
❑ The Security Officer has a documented job description	Albert Strong
❑ Establish a Security Review Board	Albert Strong
❑ Members of the Security Review Board are appointed by the Security Officer	Albert Strong
❑ The SRB will meet at least Quarterly to discuss security issues	Albert Strong
❑ Maintain formal job descriptions for all key roles	Albert Strong
❑ Ensure there are appropriate segregation of duties between key roles	Albert Strong
❑ Review and update job descriptions annually	Nimrod Vered
❑ Ensure key responsibilities are in each job description	Albert Strong
❑ Ensure security responsibilities are in each job description	Albert Strong
❑ Job description management process should have an owner	Nimrod Vered

Key Roles

Job descriptions Owner is the Chief Information Security Officer – Albert Strong

Uplevel utilizes highly professional employees and contractors for its senior level IT support. The following roles are described in individual job descriptions and are fulfilled by the employee or contractor named.

Key Roles	
CEO	Joe Levy
CTO	Nimrod Vered
CISO	Albert Strong
Cloud Computing Engineer	Dave Mathews
Senior Network Architect	Brian park
Senior Network Engineer	Dave Mathews
Database Administrator	Brian park
Application Support Analyst	Dave Mathews
Software Product Owner	Brian park
Software/Application Developer	Dave Mathews
Software Engineer	Brian park
Software Quality Assurance Analyst	Dave Mathews
Senior Web Developer	Brian park
Webmaster	Dave Mathews

Workplace Conduct Standards

Workplace Conduct Standards controls apply to the measures Uplevel takes to ensure our employees and contractors are aware of and understand the rules, regulations, and policies governing their workplace and industry. These controls ensure that employees are aware of appropriate behavior in the workplace, the appropriate process for most standard tasks, and the appropriate means of filing a grievance or recording a violation of rules and policies.

It is the policy of Uplevel that Workplace Conduct Standard Policies are maintained and updated annually.

Key Security Controls	**Responsible Party**
❑ Workplace Conduct Standard Policies are maintained and updated annually.	Albert Strong
❑ Maintain employee confidentiality agreement	Albert Strong
❑ New employees are required to sign a confidentiality agreement	Albert Strong
❑ Ensure the confidentiality agreement includes an intellectual property clause	Albert Strong

❑ Maintain and up-to-date employee handbook	Albert Strong
❑ Employee handbook and code of ethics is acknowledged annually	Albert Strong
❑ Criminal background checks are conducted for all new employees	Albert Strong
❑ References are checked for all new employees	Albert Strong
❑ The new hire process is defined in a Onboarding Checklist	Albert Strong
❑ Termination of an employee or contractor is defined by an Offboarding Checklist	Albert Strong
❑ Annual performance reviews are conducted for all employees	Joe Levy
❑ Performance reviews are defined with a checklist or template	Joe Levy
❑ Maintain and up to date Sanctions Policy	Albert Strong
❑ Employees have a process for internal complaints	Albert Strong
❑ All employees are required to read and understood the Information Security Policy during the on-boarding process	Albert Strong
❑ All employees sign-off that they have read and understood the Information Security Policy.	Albert Strong
❑ A Workstation Hardening Checklist is enforced for all employees and contractors	Albert Strong

Organization Documentation

It is important for Uplevel to create relevant and high-quality information to support the functioning of internal controls. We make sure current and accurate information is available to relevant parties which could impact information security.

- We maintain up to date and relevant network and/or system architecture diagrams that describe our system at a high level. Architectural diagrams are updated annually
- Diagrams include firewalls, external endpoints, and internal private networks
- We provide a written list of all our services. These descriptions of systems and services are available to authorized internal and external users
- We provide a description of all technical systems -- networking, email services, data storage, software licenses, security controls, etc. and the third-party services that provide them.
- Descriptions of systems and services are available to authorized internal and external users

Key Security Controls	Responsible Party
❑ Overall description of the enterprise	Joe Levy
❑ Maintain written descriptions of products and services offered	Joe Levy

❑ Description of all technical systems -- networking, email services, data storage, software licenses, security controls, etc. and the third-party services that provide them.	Nimrod Vered
❑ Descriptions of systems and services are available to authorized internal and external users	Nimrod Vered
❑ Maintain up to date network and/or system architecture diagram.	Nimrod Vered
❑ System boundaries are documented on diagrams	Nimrod Vered
❑ Physical and logical architectural diagrams are updated annually	Nimrod Vered

Security Awareness Training

Uplevel is committed to promoting safe and informed working practices. All employees will receive security awareness training. Staff working in specialized roles will receive appropriate training relevant to their role. Relevant information security policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees' responsibility to ensure they are adequately informed of information security policies and procedures.

Training includes an overview of policies and procedures

All Uplevel employees shall be trained on an annual basis as part of the Uplevel Security Awareness program. All new users must complete security training before being granted access to key systems and/or data. Exceptions may be made at the discretion of the Security Officer. The Security Officer shall communicate Uplevel's security commitments and obligations as part of the annual security awareness training.

Key Security Controls	Responsible Party
❑ A Training Policy is created	Albert Strong
❑ All employees and contractors are required to read the company Training Policy	Albert Strong
❑ Security awareness training is given to all new employees during onboarding	Albert Strong
❑ Training includes an overview of policies and procedures	Albert Strong
❑ Security Awareness Training Content Prepared and Ready to Deliver	Albert Strong
❑ Security awareness training addresses the security policy and usage of sensitive personal information	Albert Strong

❑ Security awareness training for all employees is renewed annually	Albert Strong
❑ Security awareness training is tracked; records are kept	Albert Strong
❑ Maintain up to date security awareness documentation	Albert Strong
❑ Supplemental training (conferences or external sources) is given to key engineering or operations roles	Albert Strong

Commitment to Security

Data confidentiality, integrity, and availability are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital for the protection of systems and information authorized users who have access to Uplevel systems and information are aware of and understand how their actions may affect security.

Confidentiality – systems and information will only be accessible to authorized persons.

Integrity – the accuracy and completeness of systems and information are safeguarded.

Availability – systems and information are physically secure and will be accessible to authorized persons when required.

Authorized users referred to in this document are members of the following groups:

All parties (Either as part of a contract of employment or third-party contract) who have access to, or use of systems and information belonging to, or under the control of Uplevel including:

- Uplevel employees
- Contractors
- Full and part-time staff
- Temporary staff
- Partner organizations
- Consultants
- Any other party utilizing Uplevel resources

Uplevel will abide by all relevant legislation relating to information storage and processing. Uplevel will also comply with any contractual requirements, standards and principles required to maintain the business functions including:

- Protection of intellectual property rights;
- Protection of Uplevel records and data;
- Compliance checking and audit procedures;
- Relevant codes of connection to third party networks and services.

Key Security Controls	Responsible Party
❑ Security is included in the company's master service agreement, licenses, or terms of service documents	Joe Levy

❑ Maintain an up-to-date version of the company's SLA.	Nimrod Vered
❑ Be prepared to describe the assurances that are in place demonstrating how employees will meet security commitments made to customers	Albert Strong
❑ Availability/uptime commitments are made to customers	Nimrod Vered
❑ A privacy notice or policy is posted on the company website	Joe Levy
❑ Uplevel will abide by all relevant legislation relating to information storage and processing.	Joe Levy
❑ Uplevel will also comply with any contractual requirements, standards and principles required to maintain the business functions including:	Joe Levy
· Protection of intellectual property rights;	Joe Levy
· Protection of company records and data;	Joe Levy
· Compliance checking and audit procedures;	Joe Levy
· Relevant codes of connection to third party networks and services (APIs) are not compromised	Joe Levy

Policies and Training Available

Uplevel internally communicates information, including responsibilities for internal control and security. All employees and contractors have adequate documentation to both address information security and compliance risks. All Workforce Conduct Policies, Information Security Policies, and Training is available on Google Drive.

Key Security Controls	Responsible Party
❑ Code of conduct/employee handbook is available to download at any time	Albert Strong
❑ Training material is available for review at all times	Albert Strong
❑ Policy documents are available to employees in a centralized location	Albert Strong
❑ Procedures and checklist are available to employees in a centralized location they are stored	Albert Strong

Information Security Policy Management

This Information Security Policy and associated documentation shall be reviewed and updated where appropriate on an annual basis. Changes in law, significant security incidents, risks, and business requirements should be considered, and policies should be updated accordingly. The Security Officer owns all updates, communication, and enforcement of the information system security policy. The policy is edited by the Security Review Team and approved by the management team.

Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Uplevel assets, or an event which is in breach of policies and procedures.

Uplevel will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

Failure of employees to comply with Uplevel' Information Security Policy may lead to disciplinary action under Uplevel' disciplinary procedure.

Failure of contractors, temporary staff, partners or third party organizations to comply with Uplevel' Information Security Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

A record of corrective and preventative actions shall be maintained and shall include date of identification, description, cause, action taken, action completed and effectiveness of the Nonconformity and corrective actions.

The record of Nonconformity and corrective actions shall be maintained and reviewed by the person responsible.

Key Security Controls	Responsible Party
❑ There is an Information Security Policy governing all aspects of information security	Albert Strong
❑ Information Security Policy is reviewed and updated annually	Albert Strong
❑ An owner is defined for the Information Security Policy	Albert Strong
❑ All employees sign-off that they have read and understood the Information Security Policy during the on-boarding process	Albert Strong

Risk Assessment and Management

Uplevel will maintain an inventory consisting of all information assets which will be managed in accordance with information security policies and procedures.

Risk Management Process

Uplevel shall annually conduct an accurate and thorough risk and vulnerability analysis to serve as the basis for compliance efforts. Uplevel shall re-assess the technical and non-technical security risks to its data, the confidentiality, integrity, and availability of information, and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business practices, technological advancements, and other environmental or operational changes.

The Security Officer shall maintain records of applicable laws, regulations, commitments, SLAs, and other contractual requirements. This spreadsheet is reviewed and updated on at least a quarterly basis. The Uplevel shall comply with relevant regulations.

Risk Monitoring

Uplevel has developed a Risk Management Strategy and the risk to Uplevel systems and information will be managed under this framework. Reviews are independent, unbiased and verified by either internal audit or external parties when required.

Risk Assessment Policy

Purpose and Scope

The purpose of this policy is to define the methodology for the assessment and treatment of information security risks within the organization, and to define the acceptable level of risk as set by the organization's leadership.

Risk assessment and risk treatment are applied to the entire scope of the organization's information security program, and to all assets which are used within the organization or which could have an impact on information security within it.

This policy applies to all employees of the organization who take part in risk assessment and risk treatment.

Background

A key element of the organization's information security program is a holistic and systematic approach to risk management. This policy defines the requirements and processes for the organization to identify information security risks. The process consists of four parts: identification of the organization's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

Policy

a. Risk Assessment

1. The risk assessment process includes the identification of threats and vulnerabilities having to do with company assets.

2. The first step in the risk assessment is to identify all assets within the scope of the information security program; in other words, all assets which may affect the confidentiality, integrity, and/or availability of information in the organization. Assets may include documents in paper or electronic form, applications, databases, information technology equipment, infrastructure, and external/outsourced services and processes. For each asset, an owner must be identified.

3. The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities must be listed in a risk assessment table. Each asset may be associated with multiple threats, and each threat may be associated with multiple vulnerabilities. A sample risk assessment table is provided as part of the Risk Assessment Report Template (reference (a)).

4. For each risk, an owner must be identified. The risk owner and the asset owner may be the same individual.

   Once risk owners are identified, they must assess:

   a) Consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.

   b) Likelihood of occurrence of such a risk (i.e. the probability that a threat will exploit the vulnerability of the respective asset).

   c) Criteria for determining consequence and likelihood are defined in Tables 3 and 4.

b. Risk Acceptance Criteria

1. Risk values 0 through 2 are considered to be acceptable risks.

2. Risk values 3 and 4 are considered to be unacceptable risks. Unacceptable risks must be treated.

c. Risk Treatment

1. Risk treatment is implemented through the Risk Treatment Table. All risks from the Risk Assessment Table must be copied to the Risk Treatment Table for disposition, along with treatment options and residual risk. A sample Risk Treatment Table is provided in reference (a).

2. As part of this risk treatment process, the CEO and/or other Uplevel managers shall determine objectives for mitigating or treating risks. All unacceptable risks must be treated. For continuous improvement purposes, managers may also opt to treat other risks for company assets, even if their risk score is deemed to be acceptable.

   a. Treatment options for risks include the following options:

   b. Selection or development of security control(s).

      i. Transferring the risks to a third party; for example, by purchasing an insurance policy or signing a contract with suppliers or partners.

3. Avoiding the risk by discontinuing the business activity that causes such risk.

4. Accepting the risk; this option is permitted only if the selection of other risk treatment options would cost more than the potential impact of the risk being realized.

a. After selecting a treatment option, the risk owner should estimate the new consequence and likelihood values after the planned controls are implemented.
    i. Regular Reviews of Risk Assessment and Risk Treatment

b. The Risk Assessment Table and Risk Treatment Table must be updated when newly identified risks are identified. At a minimum, this update and review shall be conducted once per year. It is highly recommended that the Risk Assessment and Risk Treatment Table be updated when significant changes occur to the organization, technology, business objectives, or business environment.
    i. Reporting

c. The results of risk assessment and risk treatment, and all subsequent reviews, shall be documented in a Risk Assessment Report.

Fraud Policy

BACKGROUND

The corporate fraud policy (incorporated as part of the Risk Management Section of the Information Security Policy) is established to facilitate the development of controls that will aid in the detection and prevention of fraud against UPLEVEL. It is the intent of UPLEVEL to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.

SCOPE OF POLICY

This policy applies to any irregularity, or suspected irregularity, involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with UPLEVEL. Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the company.

POLICY

Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities. Fraud is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. Each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity. Any irregularity that is detected or suspected must be reported immediately to the Chief Information Security Officer, who coordinates all investigations with the Legal Department and other affected areas, both internal and external.

ACTIONS CONSTITUTING FRAUD

The terms defalcation, misappropriation, and other fiscal irregularities refer to, but are not limited to:

•Any dishonest or fraudulent act

•Misappropriation of funds, securities, supplies, or other assets

•Impropriety in the handling or reporting of money or financial transactions

•Profiteering as a result of insider knowledge of company activities

•Disclosing confidential and proprietary information to outside parties

•Disclosing to other persons securities activities engaged in or contemplated by the company

•Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the company. Exception: Gifts less than $50 in value.

•Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment; and/or

•Any similar or related irregularity

OTHER IRREGULARITIES

Irregularities concerning an employee's moral, ethical, or behavioral conduct should be resolved by UPLEVEL management. If there is any question as to whether an action constitutes fraud, contact the Chief Information Security Officer for guidance.

INVESTIGATION RESPONSIBILITIES

UPLEVEL management has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, UPLEVEL will issue reports to appropriate designated personnel and, if appropriate, to the Board of Directors. Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with legal counsel and senior management, as will final decisions on disposition of the case.

CONFIDENTIALITY

UPLEVEL treats all information received confidentially. Any employee who suspects dishonest or fraudulent activity will notify UPLEVEL immediately, and should not attempt to personally conduct investigations or interviews/interrogations related to any suspected fraudulent act (see REPORTING PROCEDURE section below).Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the company from potential civil liability.

AUTHORIZATION FOR INVESTIGATING SUSPECTED FRAUD

Members of the Investigation Team at UPLEVEL will have:

•Free and unrestricted access to all Uplevel any records and premises, whether owned or rented;

•The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

REPORTING PROCEDURES

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way. An employee who discovers or suspects fraudulent activity will contact the UPLEVEL immediately. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the Investigations UPLEVEL or the Legal Department. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: "I am not at liberty to discuss this matter." Under no circumstances should any reference be made to "the allegation," "the crime," "the fraud," "the forgery," "the misappropriation," or any other specific reference. The reporting individual should be informed of the following:

•Do not contact the suspected individual in an effort to determine facts or demand restitution.

•Do not discuss the case, facts, suspicions, or allegations with any-one unless specifically asked to do so by UPLEVEL.

TERMINATION

If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by the designated representatives from UPLEVEL Management and, if necessary, by outside counsel, before any such action is taken. The UPLEVEL has the authority to terminate an employee.

The policy will be reviewed annually and revised as needed.

Key Security Controls	Responsible Party
❑ A master inventory list of system components and assets is created and maintained	Albert Strong
❑ Data and asset inventories are updated annually	Albert Strong
❑ Maintain an up-to-date version of the Information Asset inventory	Albert Strong
❑ All Information Assets have an assigned owner	Albert Strong
❑ A data inventory is created listing and describing key classes of data managed	Albert Strong
❑ Maintain an up-to-date version of the data inventory	Albert Strong
❑ A formal risk assessment and management process is documented	Albert Strong
❑ Risk are identified and ranked in terms of (RISK = Impact * Likelihood)	Albert Strong
❑ Maintain an up-to-date version of the company's risk assessment policy and procedure	Albert Strong
❑ Maintain an up-to-date version of the company's Information Asset Based Risk Register	Albert Strong
❑ Risk assessment includes risk of fraud	Albert Strong
❑ Risk assessment includes business risk and business impact	Albert Strong
❑ Security topics and risk are regularly discussed in management meetings	Albert Strong
❑ Meeting agenda/notes document risks that are discussed	Albert Strong
❑ Risk mitigate and control decisions are prioritized based on the risk assessment	Albert Strong
❑ Formal risk assessment is conducted annually using the Risk Register	Albert Strong
❑ Control-self-assessment, reviews, and/or internal audits are performed quarterly	Albert Strong
❑ Risk assessments consider changes in the regulatory environment	Albert Strong

Penetration and Vulnerability Testing

A penetration test, also known as a pen test, or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

The process typically identifies the target systems and a goal, then reviews available information and undertakes various means to attain that goal. A penetration test can help determine whether a system is vulnerable to attack if the defenses were sufficient, and which defenses (if any) the test defeated.

Key Security Controls	Responsible Party
❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	Nimrod Vered
❑ External penetration testing/vulnerability assessments are conducted annually	Nimrod Vered
❑ All medium, high, and critical finding of vulnerability and penetration test are remediated in a timely manner	Nimrod Vered
❑ Our organization has general liability insurance/cyber insurance	Nimrod Vered

Control Monitoring

Uplevel reserves the right to monitor the use of systems and information, including email and internet usage, to protect the confidentiality, integrity and availability of Uplevel' information assets and ensure compliance with policies. Uplevel may, at its discretion, or where required by law, report security incidents to the relevant authorities for further investigation.

As part of the standard audit review process, the Security Officer will routinely assess compliance with Uplevel Security Policy and applicable controls and report matters to senior management where appropriate.

Security incidents reported through the Security Incident Management Policy and Procedures, will inform on the effectiveness of controls and assist in identifying training and awareness requirements and improvements.

System Integrity

To ensure that Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

1. FLAW REMEDIATION

The CTO shall:

a. Identify, report, and correct information system flaws.

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

c. Install security-relevant software and firmware updates within 30 days of the release of the updates.

d. Incorporate flaw remediation into the configuration management process.

e. Employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.

2. MALICIOUS CODE PROTECTION

The CTO shall:

a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

b. Update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures.

c. Configure malicious code protection mechanisms to:

i. Perform periodic scans of the information system monthly and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the security policy.

ii. Block malicious code; quarantine malicious code; send alert to administrator; [entity defined action] in response to malicious code detection.

iii. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

3. INFORMATION SYSTEM MONITORING

The CTO shall:

a. Monitor the information system to detect:

i. Attacks and indicators of potential attacks.

ii. Unauthorized local, network, and remote connections.

b. Identify unauthorized use of the information system through defined techniques and methods.

c. Deploy monitoring devices strategically within the information system to collect [entity determined essential information] and at ad hoc locations within the system to track specific types of transactions of interest to the entity.

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.

g. Provide information system monitoring information to authorized personnel or business units as needed.

4. SYSTEM-GENERATED ALERTS

The CTO shall ensure that:

a. The information system that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).

b. Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. Personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

5. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

The CTO shall:

a. Receive information system security alerts, advisories, and directives from [entity defined external organizations] on an ongoing basis.

b. Generate internal security alerts, advisories, and directives as deemed necessary.

c. Disseminate security alerts, advisories, and directives to: senior management.

d. Implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

File Integrity Monitoring

Uplevel uses a combination of Cerebro (see description below) custom monitoring in our AWS S3 buckets for file integrity monitoring.

An Amazon S3 bucket name is globally unique, and the namespace is shared by all AWS accounts. This means that after a bucket is created, the name of that bucket cannot be used by another AWS account in any AWS Region until the bucket is deleted.

Amazon S3 creates buckets in a Region that is specified by Uplevel.

Objects that belong to a bucket that Uplevel creates in a specific AWS Region never leave that Region, unless we explicitly transfer them to another Region.

Identity and access management in Amazon S3

By default, all Amazon S3 resources—buckets, objects, and related subresources (for example, lifecycle configuration and website configuration)—are private: only the resource owner, an AWS account that created it, can access the resource. The resource owner can optionally grant access permissions to others by writing an access policy.

Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies attached to resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. Policies can also be attached such as access policies to users in our account. These are called user policies. Amazon S3 allows the choice to use resource-based policies, user policies, or some combination of these to manage permissions to the Amazon S3 resources.

Cerebro

Cerebro is the name of a system Uplevel developed internally and originally. It is a logging and alerting system.

Cerebro refers to a set of 'serverless' scripts that are triggered upon changes to our monitoring and logging data store. The scripts are implemented via AWS Lambda functions, and are triggered by changes in Dynamodb tables via Dynamodb stream events. These scripts allow us to direct custom notifications to specific Slack channels, as well as other notification systems if necessary. We use this for logging and alerting on a wide variety of system events including: data processing, user logins, and custom user feedback requests.

There are three steps to file integrity monitoring:

1. **Establishing a baseline for files:** Before actively monitoring files for changes, Uplevel establishes a reference point against which alterations can be detected. The standard takes into account the version, creation date, modification date, and other data that can provide assurance that the file is legitimate.
2. **Monitoring changes:** With a detailed baseline, Uplevel will then monitor all designated files for changes. We can augment our monitoring processes by auto-promoting expected changes, thereby minimizing false positives.
3. **Sending an alert:** If their file integrity monitoring solution detects an unauthorized change, Cerebro will send out an alert to the relevant personnel who can fix the issue.

Key Security Controls	Responsible Party
❑ A SOC 2 internal audit by a Certified Public Accounting firm will performs control assessments on an annual basis and communicates results to management	Nimrod Vered
❑ Control self-assessments are performed on a quarterly basis by process owners and results are communicated to management	Nimrod Vered
❑ A person within the company is named responsible for responding if the website or application goes down	Nimrod Vered
❑ Log and alerting processes are reviewed on a semi-annual basis	Nimrod Vered
❑ Admin, application, and security event logs are included in the review	Nimrod Vered
❑ Log and alert reviews are documented within the change management/ticketing application	Nimrod Vered
❑ Production environment configurations/defaults reviews are performed semi-annually	Nimrod Vered
❑ Configuration/defaults reviews are documented within the change management/ticketing application	Nimrod Vered

Logical Security

Logical Security consists of software safeguards for an organization’s systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. It is a subset of computer security.

Key Security Controls	Responsible Party
❑ Production systems and servers have been hardened to ensure an appropriate level of security against a documented standard	Nimrod Vered
❑ Scans are conducted on production systems and servers to validate the hardening is successful	Nimrod Vered
❑ Maintain an up-to-date list of what practices/standards that are used in the hardening process	Nimrod Vered
❑ SSH service is accessible to only a pre-approved/whitelist IP addresses or segments	Nimrod Vered
❑ VPN or SSH jump-hosts are required for an admin to connect to the production network	Nimrod Vered
❑ Production systems are monitored by intrusion detection software	Nimrod Vered

Access Authorization

To gain access to specific systems and information, a member of staff will need to follow a formal application process. Users will need to apply to the Chief Technology Officer using the appropriate completed forms.

- Generic logons are not generally permitted across Uplevel; however, use of generic accounts under exceptional 'controlled' circumstances is permitted. Generic accounts must be approved by the Security Officer.
- The appropriate level of access to systems and information will be determined upon the prospective users required business need, job function and role.
- If authorization to use systems and information is granted, unique logon credentials and password will be provided to the applicant. Further instruction on how to maintain the security of systems and information with due regard to the procedures below may be given.
- Access for remote users shall be subject to authorization by the Chief Technology Officer. No uncontrolled external access shall be permitted to any network device or networked system.

Systems/Information Deregistration

- If a member of staff changes role or their contract is terminated, their manager should apply to have the users access to the system/information reviewed or removed as soon as possible.
- If a member of staff is deemed to have violated any of the Information Security policies or procedures, potentially jeopardizing the availability, confidentiality or integrity of any systems or information, their access rights to the system/information should be reviewed by the system owners.
- If a specific access limit is exceeded or control circumvented several times by a user the manager should review the access rights of the user and if necessary remind the user of the relevant access and security.
- If a number of unsuccessful logon attempts are exceeded, the user will be informed that they need to contact the system owners to ask for access rights to be re-established. In these circumstances, access rights may need to be reviewed.
- If it is deemed that it is no longer appropriate or necessary for a user to have access to systems and/or information, then the user's manager will need to inform the owners of the system/information that access rights should be altered/removed immediately.
- If any system/information rights are altered or removed, the relevant documentation will need to be updated accordingly.

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the Security Officer by indicating "Remove Access" on the employee's System Access Request Form. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the Security Officer of the employee's last scheduled work day so that their user account(s) can be configured to expire and they are void of access to all customer information and Uplevel systems from that day forward.

The employee's department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as Uplevel equipment and property is returned to Uplevel prior to the employee leaving Uplevel on their final day of employment.

Key Security Controls	Responsible Party
❑ Maintain a list of all the individuals who have the responsibility of creating and managing accounts	Nimrod Vered
❑ A centralized place has been created where new accounts and account changes can be requested (ticket system / email box / form)	Nimrod Vered
❑ Maintain a list of all the individuals who have the responsibility of approving new system accounts Administrative access on systems has to be approved and must only be limited to only a few individuals	Nimrod Vered
❑ Approvals for new or changed system access is documented	Nimrod Vered
❑ All account sharing is prohibited	Nimrod Vered
❑ All user accounts are disabled timely upon termination of employment	Nimrod Vered
❑ A streamline communication channel is defined to quickly notify administrators upon employee termination	Nimrod Vered
❑ Maintain an up-to-date document describing the termination/off boarding process	Nimrod Vered

Authentication

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- All users shall have unique system ids; all generic ideas should have an owner with a designated backup.
- Users shall be responsible for the use and misuse of their individual logon ID.
- All user login IDs are audited at least twice yearly
- All inactive logon IDs are revoked.

The Uplevel Human Resources representative notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

Passwords

Where possible and applicable, passwords will be managed by LastPass password tool on company owned workstations.

User IDs and passwords are required in order to gain access to all Uplevel systems, networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess.

Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Where technically feasible, password configurations on systems should be set to:

- Enforce password history 10 passwords remembered
- Maximum password age 180 days
- Minimum password age 2 days
- Minimum password length 10 characters
- Account lockout threshold 5 invalid logon attempts
- Reset account lockout counter after 30 minutes
- Users are prompted to change password at logon 7 days prior to the existing one expiring.
- Passwords must meet complexity requirements – this forces the use of passwords which must contain at least three of the following five elements:
    - Numeric – (0-9)
    - Uppercase – (A-Z)
    - Lowercase – (a-z)
    - Special Characters (?,!, @, #, %, etc…)
    - Spaces

Password Protection Standards

Do not use the same password you use for Uplevel accounts as for other non-Uplevel access (e.g., personal accounts, personal banking, etc.). Where possible, do not use the same password for various Uplevel access needs. For example, where applications do not utilize authenticated logons, choose different passwords for separate systems.

Do not share Uplevel passwords with anyone. All passwords are to be treated as sensitive, Confidential Uplevel information.

List of "Don’ts":

- Don't reveal a password over the phone to ANYONE
- Don’t write passwords down and store them anywhere in the office
- Don't reveal a password in an email message
- Don't reveal a password to your manager
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my last name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Additional Information

If someone demands a password, refer them to this document and request that they contact the Security Officer.

Do not store passwords in a file on ANY computer system (including mobile devices or similar) without encryption.

If an account or password is suspected to have been compromised, report the incident as soon as possible to the Security Officer. Immediately change any/all passwords which may have been compromised.

Password cracking or guessing may be performed on a periodic or random basis during audit penetration tests involving 3rd party companies. If a password is guessed or cracked during one of these scans, the user will be required to change it immediately. All audit penetration tests must be approved by the Security Officer prior to the work commencing.

Key Security Controls	Responsible Party
❑ All authentication flows are encrypted - internally	Nimrod Vered
❑ All authentication flows are encrypted - customers	Nimrod Vered
❑ All users are required to have a unique ID	Nimrod Vered
❑ All systems and service accounts have a documented owner	Nimrod Vered
❑ All user login IDs are audited at least twice yearly	Nimrod Vered
❑ All inactive logon IDs are revoked.	Nimrod Vered
❑ Two Factor Authentication(2FA) is enabled on all systems that support it	Nimrod Vered
❑ 2FA is required before an administrator or engineer can connect to the production environment	Nimrod Vered
❑ Where possible and applicable, passwords will be managed by LastPass password tool on company owned workstations.	Nimrod Vered
❑ Password complexity and length requirements are enabled on all systems that do not utilize 2FA	Nimrod Vered

Role-based Access Control

Information resources are protected using role-based access control systems. Access to confidential information is only given to users on a need to know basis. Users are given the minimum necessary to perform their job responsibilities.

Rules for access to resources have been established by the Chief Information Security Officer who is responsible for the resources. Access is granted only by the completion of a System Access Request Form. This form must be used for access to any system or location that might contain any sensitive, confidential information, including ePHI.

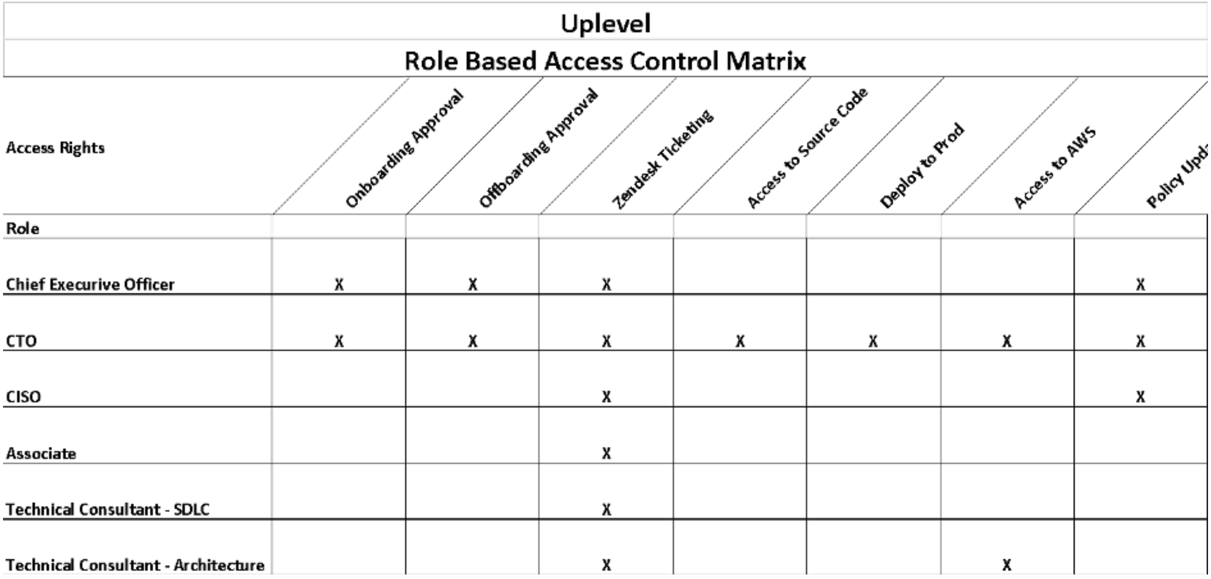
All newly provisioned, modified, or account removal must be made in the form of an access change request, be documented, and approved by the Chief Information Security Officer, or designee.

User Entitlement Reviews

If an employee changes positions at the Uplevel, employee’s new supervisor or department head shall promptly notify the Security Officer of the change of roles by indicating on the System Access Request Form both the roles or access that need to be added and the roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions.

The effective date of the position change should also be noted on the Form so that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

On a semi-annual basis, the Security Officer shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data.



Uplevel

Role Based Access Control Matrix

Access Rights	Onboarding Approval	Offboarding Approval	Zendesk Ticketing	Access to Source Code	Deploy to Prod	Access to AWS	Policy Upd
Role							
Chief Execurive Officer	X	X	X				X
CTO	X	X	X	X	X	X	X
CISO			X				X
Associate			X				
Technical Consultant - SDLC			X				
Technical Consultant - Architecture			X			X	

Key Security Controls	Responsible Party
❑ Roles and access rights are reviewed on all key production/operational systems, and physical offices semi-annually	Nimrod Vered
❑ Maintain a list of all individuals who are responsible for access rights/role reviews	Nimrod Vered
❑ Documentation is kept as evidence of the most recent access/role review	Nimrod Vered

❑ If an employee changes positions at Uplevel, employee’s new supervisor or department head shall promptly notify the Security Officer	Nimrod Vered
❑ Role-based access control is utilized on all systems that support it	Nimrod Vered

Access Restrictions

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual.

All employees must recognize the sensitive nature of data maintained by the Uplevel and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Uplevel policy and will result in personnel action and may result in legal action. Confidential information shall be encrypted at all possible times.

Employees without pre-authorized access should notify the Security Officer if they receive sensitive information.

Key Security Controls	Responsible Party
❑ Backend access to production data is limited to the Chief Technology officer and his designees.	Nimrod Vered
❑ Access to customer data is restricted through application-level controls with roles and/or permissions	Nimrod Vered
❑ Application-level controls can be easily demonstrated with a screenshot	Nimrod Vered
❑ Sensitive information is never printed, or when necessary, marked as ‘Confidential’ in the footer	Nimrod Vered
❑ Printed sensitive information is physically secured	Nimrod Vered

Data Encryption

Encryption is applied to all authorized data storage devices attached to desktop, laptop, or tablet computers. In certain cases, it may not be feasible for certain devices to be encrypted and each exception to a device will be given full and careful consideration as to its use and any decision made will be based on best practice and business need.

All backend systems shall encrypt sensitive data while at rest (e.g. databases) and in transit.

1. Overview

Uplevel “Confidential Information” and Employee, or Customer Personally Identifiable Information (“PII”) must be protected while stored at-rest and in-transit. Appropriate encryption technologies must be used to protect the Uplevel.

2. Purpose

The purpose of this policy is to provide guidance on the use of encryption technologies to protect Uplevel data, information resources, and other Confidential Information or PII while stored at rest or transmitted between parties. This policy also provides direction to ensure that regulations are followed.

3. Scope

This policy applies to all Uplevel staff that create, deploy, transmit, or support application and system software containing Confidential Information or PII. It addresses encryption policy and controls for Confidential Information or PII that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

4. Policy

A. ACCESS

The CTO or their designee shall ensure:

o Policies, procedures, scenarios, and processes must identify Confidential Information or PII that must be encrypted to protect against persons or programs that have not been granted access.

o Uplevel implements appropriate mechanisms to encrypt and decrypt Confidential Information or PII whenever deemed appropriate. Internal procedures shall specify how Uplevel transmits sensitive information as well as how often the information is transmitted.

o When encryption is needed based on data classification to protect Confidential Information or PII during transmission. Procedures shall specify the methods of encryption used to protect the transmission of Confidential Information or PII.

o Logical user access is managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials) when disk encryption is used rather than file or column level database encryption.

B. ENCRYPTION KEY LENGTH

Uplevel uses software encryption technology to protect Confidential Information or PII. To provide the highest-level security while balancing throughput and response times, encryption key lengths should use current industry standard encryption algorithms for Confidential Information or PII.

The use of proprietary encryption algorithms are not allowed unless reviewed by qualified experts outside of the vendor in question and approved by Uplevel management.

Encryption Key Policy

Uplevel uses encryption at rest and in-transit for all customer data.

As a general policy, Uplevel should not directly deal with encryption keys.

- Encryption keys should not be sent over Slack, email, or other methods of communication

- Usage of encryption keys should be gated behind some sort of identity service (Hashicorp Vault login/tokens or AWS IAM).
- Encryption keys should only be generated by managed services (eg. Hashicorp Vault or AWS KMS)
- All AWS services should have encryption turned on where applicable.

These policies help prevent the leakage of keys; by restricting the access of encryption keys to a user or token of some sort, it allows us to keep an audit trail of when and where data was accessed.

Vault

In the case of our ConnectorHub architecture, we utilize Hashicorp Vault's "encryption as a service" API. Although we allow Uplevel employees to generate a login and password for our clients, it is important to note that these are not the same as an encryption key.

A token can be revoked, for example, while keeping the encryption key intact. This allows us to rotate passwords that can gain access to the encryption key.

Vault, by design, makes it difficult to directly access the encryption key, so the risk of encryption key leakage - especially when taking advantage of their API - is relatively low.

AWS

AWS has a managed service called KMS (Key Management System). When services involving persistent data are initialized in AWS, the option to encrypt the data stored in them should always be enabled.

In general, once encryption is enabled, AWS will handle the decryption process automatically, so you should not notice any change in the behavior of services.

C. AT-REST ENCRYPTION

• Hard drives that are not fully encrypted (e.g., disks that one or more un-encrypted partitions, virtual disks) but connect to encrypted USB devices, may be vulnerable to security breach from the encrypted region to the unencrypted region. Full disk encryption avoids this problem and shall be the method of choice for user devices containing Confidential Information or PII.

• Confidential Information or PII at rest on computer systems owned by and located within Uplevel controlled spaces, devices, and networks should be protected by one or more of the following mechanisms:

o Disk/File System Encryption (e.g. Microsoft EFS technology)

o Sanitizing, redacting, and/or de-identifying the data requiring protection during storage to prevent unauthorized risk and exposure (e.g., masking or blurring PII)

o Supplemental compensating or complimentary security controls including complex passwords, and physical isolation/access to the data

o Strong cryptography on authentication credentials (i.e. passwords/phrases) shall be made unreadable during transmission and storage on all information systems

o Password protection to be used in combination with all controls including encryption o Computer hard drives and other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure upon return for redistribution or disposal

D. PORTABLE DEVICE ENCRYPTION

• Portable devices (e.g. smart-phones, flash cards, SD cards, USB file storage) represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of Confidential Information or PII are the result of stolen or lost portable computing devices. The most reliable way to prevent exposure is to avoid storing Confidential Information or PII on these devices.

• As a general practice, Confidential Information or PII shall not be copied to or stored on a portable computing device or Uplevel-owned computing device. However, in situations requiring Confidential Information or PII to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen. The following procedures shall be implemented when using portable storage:

o Hard drives (laptops, tablets, smartphones and personal digital assistants (PDAs)) shall be encrypted using products and/or methods approved by Uplevel [Insert Appropriate Roles]. Unless otherwise approved by management, such devices shall have full disk encryption with pre-boot authentication.

o Devices shall not be used for the long-term storage of any Confidential Information or PII.

o All devices shall have proper and appropriate protection mechanisms installed including approved anti-malware/virus software, personal firewalls with unneeded services and ports turned off, and properly configured applications.

o Removable media including CD's, DVD's, USB flash drives, etc. shall not be used to store Confidential Information or PII.

E. IN-TRANSIT ENCRYPTION

In-transit encryption refers to transmission of data between end-points. The intent of these policies is to ensure that Confidential Information or PII transmitted between companies, across physical networks, or wirelessly is secured and encrypted in a fashion that protects student Confidential Information or PII from a breach.

The CTO or their designee shall ensure:

• Formal transfer policies, protocols, procedures, and controls are implemented to protect the transfer of information through the use of all types of communication and transmission facilities.

• Users follow Uplevel acceptable use policies when transmitting data and take particular care when transmitting or re-transmitting Confidential Information or PII received from non-Uplevel staff.

• Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) are used to safeguard Confidential Information or PII during transmission over open public networks. Such controls include:

o Only accepting trusted keys and certificates, protocols in use only support secure versions or configurations, and encryption strength is appropriate for the encryption methodology in use.

o Public networks include but are not limited to the Internet, Wireless technologies, including 802.11, Bluetooth, and cellular technologies.

o Confidential Information or PII transmitted in e-mail messages are encrypted. Any Confidential Information or PII transmitted through a public network (e.g., Internet) to and from vendors, customers, or entities doing business with Uplevel must be encrypted or transmitted through an encrypted tunnel (VPN) or point-to-point tunneling protocols (PPTP) that include current transport layer security (TLS) implementations.

o Encryption or an encrypted/secured channel is required when users access Uplevel Confidential Information or PII remotely from a shared network, including connections from a Bluetooth device to a Uplevel PDA or cell phone.

o Secure encrypted transfer of documents and Confidential Information or PII over the internet uses current secure file transfer programs such as “SFTP” (FTP over SSH) and secure copy command (SCP).

o All non-console administrative access such as browser/web based management tools are encrypted using SSL based browser technologies using the most current security algorithm.

F. ENCRYPTION KEY MANAGEMENT

Effective enterprise public and private key management is a crucial element in ensuring encryption system security. Key management procedures must ensure that authorized users can access and decrypt all encrypted Confidential Information or PII using controls that meet operational needs. Uplevel key management systems are characterized by following security precautions and attributes:

- Uplevel uses procedural controls to enforce the concepts of least privilege and separation of duties for staff. These controls apply to persons involved in encryption key management or who have access to security-relevant encryption key facilities and processes, including Certificate Authority (CA) and Registration Authority (RA), and/or contractor staff.

- The CTO shall verify backup storage for key passwords, files, and Confidential Information or PII to avoid single point of failure and ensure access to encrypted Confidential Information or PII.

- Key management should be fully automated. The Uplevel CTO should not have the opportunity to expose a key or influence the key creation.

- Keys in storage and transit must be encrypted.

- Private keys must be kept confidential.

- Application and system resource owners should be responsible for establishing data encryption policies that grant exceptions based on demonstration of a business need and an assessment of the risk of unauthorized access to or loss of Confidential Information or PII.

The CTO or their designee shall ensure:

- Decryption keys are not associated with user accounts.

- Documentation and procedures exist to protect keys used to secure stored Confidential Information or PII against disclosure and misuse.

- Restrict access to cryptographic keys to the fewest number of custodians necessary.

- Cryptographic keys are stored in the fewest possible locations.
- Key management processes and procedures for cryptographic keys are fully documented.
- Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.

Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived. Archived cryptographic keys should only be used for decryption/verification purposes.

Cryptographic key custodians shall formally acknowledge that they understand and accept their key-custodian responsibilities.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of Uplevel operational methodology.

- Uplevel shall inventory encrypted devices and validate implementation of encryption products at least annually.
- Documentation shall exist for key management procedures.
- At-Rest encryption procedures exist and can be demonstrated.
- In-Transit encryption procedures exist and can be demonstrated.
- Exception logs exist and can be produced for those resources that are excluded from this policy.

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all Uplevel staff and contractors using Uplevel Confidential Information or PII resources.

Key Security Controls	Responsible Party
❑ All system administration is performed over encrypted connections	Nimrod Vered
❑ All browser sessions are forced to use TLS 1.2 HTTPS connections	Nimrod Vered
❑ All system API connections are encrypted	Nimrod Vered
❑ All sensitive customer data is encrypted at rest	Nimrod Vered
❑ Maintain up-to-date documentation on how customer data is encrypted at rest, and how keys are managed	Nimrod Vered

❑ All workstations/laptop drives are encrypted	Nimrod Vered
❑ All removable media is encrypted or prohibited	Nimrod Vered
❑ All email that contain sensitive information to external domains is encrypted or prohibited	Nimrod Vered

Workstation and Laptop Security

All Uplevel workstations and physical systems must be hardened before use. This includes enabling encryption, enabling operating systems level firewalls, and enabling password protection.

All users must not disable workstation auto-update. Vendor patches shall be applied at least monthly. Users are responsible for ensuring that all 3rd party software is kept up to date.

All users are required to use Firefox as a default browser. Installation of alternative browsers must have a business purpose and prior approval by the Security Officer.

All system administration and engineering must occur on Uplevel supplied workstations or laptops.

New system components (gems, software, packages, libraries, languages) must be approved by the CTO.

Also see the stand alone policy Workstation and Laptop Security Policy

Key Security Controls	Responsible Party
❑ All employees and contractors have read and signed the Workstation and Laptop Security Policy	Albert Strong
❑ All workstations and laptops have malware protection installed	Albert Strong
❑ Installation of software on workstations or laptops is prohibited except to only approved applications	Albert Strong
❑ An email system is utilized with built-in spam and malware detection	Albert Strong

Use of Removable Media and Mobile Computing Devices

This policy establishes safeguards for using removable media in conjunction with Uplevel computing resources and data. Appropriate security of all removable media, whether owned by Uplevel or by individuals, is required to prevent the spread of viruses, the loss or compromise of sensitive data, and other risks to the Uplevel network.

DEFINITIONS

Removable Media: Removable Media may be defined as any of the following

Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.

Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.

USB card readers that allow connectivity to a PC.

Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function.

PDAs, cell phone handsets, and smartphones with internal flash or hard drive-based memory that support a data storage function

Digital cameras with internal or external memory support.

Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.

Any hardware that provides connectivity to USB devices through means such as wireless (Wi.Fi, WiMAX, irDA Bluetooth, among others) or wired network access.

Mobile Computing Device: A Mobile Computing Device may be defined as any of the following whether owned by Uplevel or by Individuals.

Portable computer or laptop that connects to or contains Uplevel data

Any cellular device or tablet that is capable of storing Uplevel information including emails or other electronic correspondence

PROCEDURES and RESPONSIBILITIES

All members of the Uplevel community have a responsibility to protect the confidentiality, integrity, and availability of Uplevel information collected, processed, transmitted, stored, or transmitted on mobile computing devices and removable media. The use of such data is provided to Uplevel employees as a privilege and improper storage or loss of such data could result in penalties both to the Uplevel and the individual employee responsible.

Responsibilities of End Users:

Users must ensure that the removable data storage medium and mobile computing devices are free from malicious software before connecting them to Uplevel computers or network devices

Users should never store confidential Uplevel data in removable media or on un-encrypted mobile computing devices

All removable media and mobile computing devices are required to be properly encrypted and password protected to protect in case of loss

Users should ensure that removable storage devices and mobile computing devices are stored in areas that are physically secure

If a device containing Uplevel information including email is lost or stolen, the incident must be reported to the Office of Information Technology immediately

Sanctions

Violation of the policies described herein for use of removable media and mobile computing devices are dealt with seriously. Violators may and are subject to the disciplinary procedures of the Uplevel, up to and including termination. In addition, violators may lose computing privileges. Illegal acts involving Uplevel computing and networking facilities may also be subject to prosecution by state and federal officials.

Detection and Recovery

Key Security Controls	**Responsible Party**
❑ A centralized logging system and alerting system is used	Nimrod Vered
❑ Critical system alerts result in an incident ticket being created	Nimrod Vered
❑ System configurations, settings, and defaults are backed up	Nimrod Vered
❑ Operation metrics are reviewed during management and/or team meetings	Nimrod Vered
❑ Meeting minutes and/or agendas are kept when reviewing operation metrics	Nimrod Vered

Security Based Software Development

Software Development Life Cycle

The purpose of this section is to establish a standard expectation for implementation of a Software Development Lifecycle (SDLC) that produces software that is secure, accessible, mobile ready, and compliant with Uplevel development standards, policies, and practices.

1. Scope

The scope of this policy includes all Uplevel employees, contractors, and temporary workers involved in the development of Uplevel software.

2. Background

The SDLC must address common business and development phases to be effective across the enterprise, and must address key issues of security, accessibility, mobile device access, and standards compliance.

3. Exceptions

A business case for non-compliance must be established and the request for exemption approved in advance through a risk acceptance process where the Chief Information Security Officer or authorized designee is notified and approval for the exception is granted.

4. Policy

Software development projects must address the following areas in a manner consistent with standard Uplevel business and development practices. All SDLC phases must be addressed and incorporated in a consistent manner. Agencies and developers may make necessary adaptations based on the size and complexity of projects. Policy implementation may incorporate Uplevel standards and guidelines that may be more stringent than the control points or phases identified in this SDLC.

The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software by a non-administrative personnel.

Based upon a stakeholder's initiation request, the objective of this phase is to conduct a preliminary analysis, propose alternative solutions, describe costs and benefits and submit a preliminary plan with recommendations.

Conduct the preliminary analysis: In this step, document the Uplevel's objectives and the nature and scope of the problem under study.

Describe the costs and benefits. Look at tangible costs versus tangible and intangible benefits. Address the benefits of new development versus improvements to existing systems, adaptations of other Uplevel systems, doing nothing, or purchasing a commercial solution.

Identify risks: Every project or task has risks. Cost, time, implementation, security, privacy, and regulatory risks may be identified. Risk reduction and mitigation plans are to be considered as part the preliminary analysis of any development effort.

Budget approval: Obtain management and financial approval for the project and add pertinent business case documentation as required.

Phase 2: Systems analysis, requirements definition

Defines project goals into defined functions and operation of the intended application. Analyzes end-user information needs. Address requirements for security, mobility, accessibility, and platform use expectations.

Phase 3: Systems design

Describes desired features and operations in detail, including screen layouts, business rules, process diagrams, pseudo code and other documentation. Depending upon the size of the project, prototyping is useful in this stage. Larger complex projects require more definition and more controls. Smaller projects may move directly to faster methodologies.

Phase 4: Development

Actual development of code, preferably in functional components that can be tested separately. Apply company standards such as:

Accessibility

Privacy

Security

Mobility and Usability

Web Standards

Phase 5: Integration and testing

Brings all the pieces together into a testing environment, then checks for errors, bugs and interoperability, accessibility, mobility, performance, standards compliance, and an independent security review.

Accessibility Testing

Environment, Integration, and System Testing

User Interface and Unit Testing

Load Testing and Performance Tuning

Privacy Policy Compliance

Security Code Testing

Mobility and Usability Testing

Standards Compliance Testing

Phase 6: Acceptance, installation, deployment

The final stage of initial development, where the software is put into production and runs actual business. This is the final checkpoint on architectural compliance, application and hosting security. Development (DEV), Acceptance (AT), and Production (PROD) environments must be physically separate instances on different servers.

Phase 7: Maintenance plan

What happens during the rest of the software's life: changes, corrections, additions, moves to a different hosting platform, decommissioning, and more.

5. Enforcement

Software development managers and their contractors and staff are accountable for SDLC implementation. Violation of this policy may be the basis for discipline including but not limited to termination. Individuals found to have deliberately violated this policy may also be subject to legal penalties as may be prescribed by Uplevel and/or federal statute, and/or regulation. Funding of future software development projects may be withheld if the requirements of these processes are not followed.

Key Security Controls

- ❑ Confidentiality, integrity, and availability of data is addressed during the system development lifecycle
- ❑ All engineers are aware they have the responsibility of bringing up security concerns during the software development process

- ❑ Define when changes to a system with a direct security impact receives special attention

All changes to system code infrastructure need to be assessed for impact on the security of data and information as part of standard risk assessments

SDLC Quality Assurance

Testing starts once the coding is complete and the modules are released for testing. In this phase, the developed software is tested thoroughly, and any defects found are assigned to developers to get them fixed.

Retesting, regression testing is done until the point at which the software is as per the customer's expectation. Testers refer SRS document to make sure that the software is as per the customer's standard.

Key Security Controls	Responsible Party
❑ Confidentiality, integrity, and availability of data is addressed during the system development lifecycle	Nimrod Vered
❑ All engineers are aware they have the responsibility of bringing up security concerns during the software development process	Nimrod Vered
❑ Changes to a system with a direct security impact receives special attention according to defined criteria	Nimrod Vered
❑ Changes require peer review and approval before being deployed into production	Nimrod Vered
❑ Change control software is used for all changes	Nimrod Vered
❑ Employees can report bugs through the change management ticketing system	Nimrod Vered
❑ Source code is restricted to only authorized users	Nimrod Vered
❑ All engineers are made aware of the OWASP and secure development coding practices and developers, implementation specialist, system operation specialist are required to undergo security training on a regular basis	Nimrod Vered
❑ Open-source software is approved before being used in production	Nimrod Vered
❑ Define who reviews and approves open-source software and library usage	Nimrod Vered

Change Management

To ensure that Uplevel is tracking changes to systems, and workstations including software releases and software vulnerability patching in information systems. Change tracking allows efficient troubleshooting of issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

1. Overview

In accordance with mandated organizational security requirements set forth and approved by management, Uplevel has established and implemented a formal Change Management policy (CMP) and supporting procedures. This policy is to be evaluated on an annual basis for ensuring its adequacy and relevance regarding Uplevel's needs and goals.

2. Purpose

This policy and supporting procedures are designed to provide Uplevel with a documented and formalized Change Management policy that is always to be adhered to and utilized throughout the organization . Compliance with the Uplevel policy and supporting procedures helps ensure the security and availability of the Uplevel platform resources and supporting assets. Additionally, the documented Change Management policy and supporting procedures establishes strict guidelines for requesting, initiating, and undertaking changes to various environments and platforms and their supporting system resources. This allows all changes to be approved, documented in a comprehensive manner, authorized, and completed in a prioritized manner.

3. Scope

This policy and supporting procedures encompasses all critical system resources and supporting assets that are essential to the security and availability of the Uplevel platform; including but not limited to:

- Software applications and services developed by Uplevel to include testing and production environments
- Production system infrastructure required to operate the Uplevel platform
- All resources storing customer data such as Relational Databases, Blob Storage etc.
- Any other systems or resources that may impact security and availability.

4. Out of Scope

There are many IT tasks performed at the company that do not fall under the policies and procedures of the CMP. Tasks that require an operational process, but are outside the initial scope of the CMP includes:

1. Changes to non-production elements or resources
2. Contingency/Disaster Recovery

5. Policy

All Uplevel employees and contractors must adhere to the Change Management policy and following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

1. All software bug fixes with an impact of critical or major and enhancements to the Uplevel platform or production system changes must have documented approval by the Product Steering Group.
2. Any Uplevel employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log via Jira all changes made to the system.
3. A rollback process must be created and defined prior to platform deployment and a backup of the previous deployment maintained for a minimum of two weeks in the event of unintended adverse consequences within the system.
4. Changes to user rights and access on key production systems require approval from the CTO.
5. Tests of key functions/methods must be written and deemed passing before being deployed to production.
6. All software changes or enhancements to production must be peer reviewed and have CTO approval.
7. All changes on key systems should be evaluated to whether there is a significant impact to confidentiality, integrity, and availability.
8. Authorization must be received from the CTO and documented through the go-no-go form prior to Uplevel platform or production system architecture deployment.
9. All vendor changes deployed outside of a regularly scheduled deployment requires a full backup of production to be retained until the next scheduled deployment.
10. Security source code scanning must be performed on staging with all high and medium impact changes remediated prior to deployment.
11. All changes must be communicated to all relevant parties including affected clients and employees.

6. Overview of Change Workflow

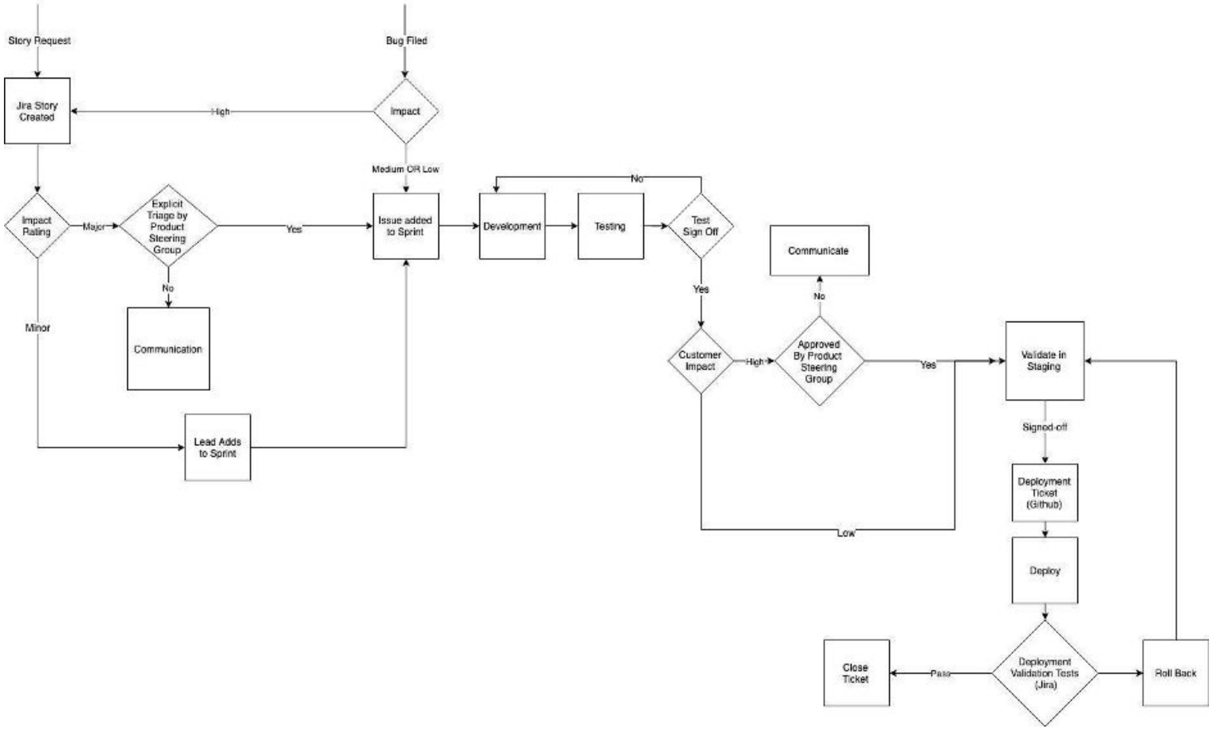
6.1. Types of Change

The following two types of change management requests are to be used: (1). Changes that are routine, planned, have been scheduled accordingly, and that can be conducted within a reasonable and agreed upon timeframe. (2). Changes that are deemed "emergency" in nature, specifically, those that are critical and have the potential to significantly impact operations within any given environment. While routine changes are required to undertake all mandated steps, the same is to be said for emergency change, but in an expedited manner. T*his means that emergency changes must still be requested, reviewed and approved before the change itself can be initiated.*

6.2. Types of Process

There are two types of change processes at Uplevel: (1) Uplevel platform software and (2) Production System and Infrastructure changes. Uplevel software changes involve all code changes on development and production systems for core software solution. Production System changes involve all changes to the production systems that support the core application contained within the Azure environment. While both processes require all the key change management steps: priority and impact analysis, approval, documentation, testing, peer review, authorization, and post-deployment security testing, each process has unique ways in which these tasks are accomplished. The forms utilized, and approval steps will be unique as outlined below.

6.3. Uplevel Platform Change Process Overview


Story Request
Bug Filed
Jira Story Created
High
Impact
Medium OR Low
Impact Rating
Major
Explicit Triage by Product Steering Group
Yes
Issue added to Sprint
Development
Testing
No
Test Sign Off
No
Communication
Minor
Lead Adds to Sprint
Yes
Communicate
No
Customer Impact
High
Approved By Product Steering Group
Yes
Validate in Staging
Low
Signed-off
Deployment Ticket (Github)
Deploy
Close Ticket
Pass
Deployment Validation Tests (Jira)
Roll Back

7. Process

7.1. Approval

Impact Rating for every new Story is assessed by a Technical Lead or higher. Following individuals can provide an Impact Rating for a new Change:

Position	Current Member
CTO	Nimrod Vered
Technical Lead	Brian Park
Technical Lead	April Bingham
Technical Lead	Anand Logannathan
Head of Data Science	Stef

Explicit Triage and Customer Impact Analysis before Deployment is done by the Product Steering Team:

Position	Current Member
CEO	Joe Levy
CTO	Nimrod Vered
Product	Dave Matthews
Head of Data Science	Stef

7.2. Change Initiation

CMP begins with the creation of a request for change within Jira. It ends with the satisfactory implementation of the change and the communication of that change to all interested parties. The CTO will communicate to the affected parties notice of rejection. The Technical Lead will create the deployment ticket, which will be linked to a collection of change request tickets.

7.3. Change Management Record

A vital component of any successful change management platform is the ability to effectively document all critical information for a given change. Specifically, this means utilizing one of two Jira change request tickets that captures and records such information. This allows all authorized individuals to input vital information as needed. Moreover, the record is to be archived indefinitely, available as needed for any number of reasons, such as for audits, investigate reasons, operational activities, etc. The following ticket types along with the required attributes, fields, and other supporting information to be included are:

Change Request Ticket:

1. Change Type: Software (default) /Infrastructure/Other
2. Priority: Highest, High, Medium (default), Low, Lowest [these are the standard Jira values]
3. Security Impacting: Yes/No (default)
4. Security Impact: (free form, blank by default)
5. Change involves Authentication, Encryption, User/Role rights, and data Separation: Yes/No (if Yes automatic assignment of Major to #10)

6. Change Impact Level: A change incorporating authentication, encryption, User/Role rights, or data separation, Major, Medium, Minor (default)

Deployment Ticket:

- Release Notes (Explicitly listed in Github Merge Record)
- Manual and Automated Test Results from Staging (Explicitly Uplevel in Github Merge Record)
- Deployment Approval (Software or Infrastructure) in Comments (Explicitly Uplevel in Github Merge Record)
- Rollback if applicable (Instructions in Github Merge Record)
- Deployment Target Environment
- Deployment Type
- Planned Deployment Date and Time
- Branch
- Any other comments.

7.4. Change Management Priority Levels

The following change management priority levels, along with a brief description of each, are to be utilized:

7.4.1. Urgent (1)

These types of changes require immediate attention and take priority over all other projects, due in large part because non-implementation of a change request with a priority level of 1 can cause serious operational problems and constraints for a very large number of users. As such, all necessary resources - operational and technical - are to be allocated to changes with a level 1 priority. Additionally, the change request itself must utilize a Change Management Record and be logged accordingly within the Change Management System (Jira).

7.4.2. High (2)

These types of changes also require immediate attention, second only to changes with a priority level of 1. Thus, all available resources - operational and technical - are to be allocated to changes with a level 2 priority. Additionally, the change request itself must utilize a Change Management Record and be logged accordingly within the Change Management System (Jira).

7.4.3. Medium (3)

These types of changes are submitted and are undertaken as part of the daily change management process whereby change requests are worked as they are submitted. No defined urgency is placed on change requests with a level 3 priority. Additionally, the change request itself must utilize a Change Management Record and be logged accordingly within the Change Management System (Jira).

7.4.4. Low (4)

These types of changes are also undertaken as part of the daily change management process whereby change requests are worked as they are submitted. No defined urgency is also assigned to change requests with a level 4 priority, and often these changes are undertaken with the next scheduled release, upgrade, enhancement, etc. or a major product or service. These changes do not require the use of a Change Management Record and do not need to be logged within the Change Management System (Jira).

7.5. Change Impact Assessment

Each change must be assessed to determine the impact on the security and availability of the systems and resources being affected by the change. Some examples of changes that impact security are but not limited to authentication, encryption, User/Role rights, and data separation change. This assessment will be captured through a Change Management Approval Record which will be attached to the Change Management Record (Jira ticket). The following change management impact levels, along with a brief description of each, are to be utilized:

7.5.1. Critical (1)

These types of change requests impact the security and availability of critical system resources that support enterprise-wide daily operational activities and a large user base, either internally, and/or from a customer facing perspective and must be deployed to production earlier than the next regularly scheduled deployment.

7.5.2. Major (2)

These types of change requests often impact the security and availability of critical system resources that support enterprise-wide daily operational activities and a large user base, either internally, and/or from a customer facing perspective and will be deployed within the next regularly scheduled deployment.

7.5.3. Medium (3)

These types of change requests often impact the security and availability of critical system resources that support enterprise-wide daily operational activities and but only for a limited user base, either internally, and/or from a customer facing perspective.

7.5.4. Minor (4)

These types of change requests impact non-critical system resources that support enterprise-wide daily operational activities. Additionally, they may impact critical systems, but not in a manner that disrupts the security and availability of system resources.

7.6. Change Management System

An important element of the entire change management process is the ability to effectively store all Change Management Records that are opened and used for making changes. This is effectively known as the Change Management System and is to be utilized as necessary by all personnel throughout the entire change management lifecycle. Uplevel has mandated the use of the Jira enterprise ticketing system as its Change Management System. By using both a Change Management Record and a Change Management System, the entire change management lifecycle is thus documented in a comprehensive manner.

7.7. Local Testing Checklist

This is a list of activities that an Engineer must have completed before asking for a Peer Review.

1. All Unit Tests Must Pass
2. All Basic Validation Tests Must Pass

3. All Security Tests Must Pass

UI only changes can be tested in a local environment. Backend/Server changes have to be tested in a Prod-like Environment (multibox hosted environment that resembles our customer environment).

7.8. Attributes Required in Peer Review (Pull Request)

These are the list of things that every Peer Review (Pull Request in Github) must include.

1. Local Test Results
2. Local Sonar Static Analysis Results
3. Any impact on Authentication, Encryption, User/Role rights, and data Separation

7.9. Pre-deployment Checklist

This is a list of statements that must be true before we can proceed with Deployment.

1. Local Testing Passed
2. Basic Validation Tests have all passed in Staging
3. Code change is not coupled with an infrastructure change
4. Content required for deployment is up to date

7.10. Titles, Roles, and Responsibilities

A critical component of the entire change management lifecycle is ensuring that all appropriate parties are assigned designated titles, roles, and responsibilities, such as the following:

7.10.1. Change Management Originator and Requester (CMOR)

The individual who requests a change. This can include authorized internal personnel, along with applicable third-parties, such as clients and vendors.

7.10.2. Software Architect

The individual responsible, along with the CMM, for reviewing the change for ensuring it meets all Uplevel goals and objectives and is commensurate with the organization's needs.

7.10.3. Technical Lead

The individual who is responsible for reviewing internal bug fix requests, assessing the impact of the change, approving medium and minor bug fix changes, and subsequently aiding and facilitating the entire change management lifecycle process, which includes corresponding with appropriate parties, ensuring the change is being worked as required, resolving any discrepancies or issues, etc.

7.10.4. Product Steering Group (PSG)

The group of individuals responsible for approving, coordinating and overseeing the change.

7.10.5. Developer

The individuals responsible for administering and undertaking all necessary processes, procedures, and related activities for the respective change itself.

Post Implementation Review

Certain major releases or System upgrades will be subject to a Post-Implementation Review.

Thisis used to evaluate the effectiveness of the system development after the system has been in production for a period of time (normally 6 months).

The objectives are to:·

- Determine if the system does what it is designed to do: ·
- Does it support the user as required in an effective and efficient manner?

The review should assess how successful the system is in terms of:·

- functionality
- performance
- cost versus benefits
- assess the effectiveness of the life-cycle development activities that produced the system.

The review results can be used to strengthen the system as well as system development procedures.

IT Acquisitions, Maintenance and Decommissioning Policy

Background

Over time, 3rd party software may be acquired. In addition, company workstations will employ laptops purchased in the open market.

Therefore, the Policy on IT Acquisitions establishes conditions under which a contemplated information technology acquisition would be subject to review by the Chief Technology Officer.

The provisions of the Policy on IT Acquisitions are subject to change with proper executive review.

Objectives

Credentials are removed, and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.

The objectives of the Policy on IT Acquisitions are threefold:

1. To ensure that IT acquisitions integrate well into UPLEVEL technology environment and facilitate the ability to carry out UPLEVEL business.
2. To ensure that any risk, security exposure or liability associated with an IT acquisition is identified and managed.
3. To ensure that UPLEVEL achieves the maximum value from any information technology investment.

Applicability

The Policy on IT Acquisitions applies to all IT purchases or acquisitions made on behalf of UPLEVEL. The policy covers planned acquisitions of information technology hardware, software, firmware and services or any combination of these things.

Policy on IT Acquisitions

Any acquisition involving the purchase or acquisition of computers, network equipment, software, applications or information technology services including but not limited to software development, installation, implementation or provision of ASP services and satisfying any one or more of the three (3) criteria listed below must be reviewed by Technology Services. The review must occur before the acquisition may take place.

The criteria:

1. The contemplated purchase duplicates functionality or services that are already available at UPLEVEL.

2. The purchase includes one or more computers that are to be maintained by Chief Technology Officer.

3. The initial value of the IT acquisition is more than $5,000 or the total-cost-of-ownership for the first 3 years.

The Process

New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point.

To initiate an IT acquisition review, the person coordinating the acquisition should create an Incident Ticket (support request) and forward it to the Chief Technology Officer.

The individual requesting the review will receive a written response which will also be maintained on file in Technology Services.

If the review process determines that the planned acquisition should not go forward, the Chief Technology Officer will work with the individual requesting the review to identify alternatives that are acceptable. In those rare instances when no agreement on an alternative can be reached, the request will be reviewed by the CEO.

Software Maintenance

This section refers to the modification of a software product after delivery to correct faults, to improve performance or other attributes.

Software maintenance is a broad activity that includes error correction, enhancements of capabilities, deletion of obsolete capabilities, and optimization. Because change is inevitable, mechanisms must be developed for evaluation, controlling and making modifications.

Software maintenance planning

An integral part of software is the maintenance one, which requires an accurate maintenance plan to be prepared during the software development. It should specify how users will request modifications or report problems. The budget should include resource and cost estimates. A new decision should be addressed for the developing of every new system feature and its quality objectives.

Software maintenance processes

1. The implementation process contains software preparation and transition activities, such as the conception and creation of the maintenance plan; the preparation for handling problems identified during development; and the follow-up on product configuration management.
2. The problem and modification analysis process, which is executed once the application has become the responsibility of the maintenance group. The maintenance programmer must analyze each request, confirm it (by reproducing the situation) and check its validity, investigate it and propose a solution, document the request and the solution proposal, and finally, obtain all the required authorizations to apply the modifications.

Hardware Maintenance and Repair

To date, the inventory of company hardware is limited to employee laptops. UPLEVEL utilizes the Apple Protection Plan for support in the event of maintenance or repair of employee workstations. This includes protections against any introduction of malware or other unauthorized software.

Decommissioning

This policy shall govern how UPLEVEL information systems, hardware, software, applications and/or databases are decommissioned in compliance with UPLEVEL records retention policies and schedules.

This policy applies to any information system, application and/or database that have been procured with UPLEVEL funds.

UPLEVEL is the primary user, or owner of the information system, hardware, software, application and/or database. The UPLEVEL CTO, when decommissioning an information system, application and/or database, may require that the records contained within the information system, application and/or database must be retained beyond the useful life of the information system, application and/or database. Prior to decommissioning an information system, hardware, software, application and/or database, the CTO will inventory the types of records contained within the said information system, application and/or database to ensure that the records contained therein will be maintained according to published UPLEVEL data management policy.

Key Security Controls	Responsible Party
❑ A change management process is in place to govern software/product and infrastructure changes	Nimrod Vered
❑ Change management procedures for infrastructure, data, and software is reviewed and updated annually	Nimrod Vered
❑ Maintain an up-to-date version of the change management policy	Nimrod Vered

❑ Change procedures are updated after a root cause analysis/quality assurance test if it is found that classes of bugs or issues are not consistently detected	Nimrod Vered
❑ Change requests are generated based on needs discovered in risk assessment processes	Nimrod Vered
❑ Notifications are sent to business operations when significant changes are implemented	Nimrod Vered
❑ The confidentiality, integrity, and availability of data is considered during all phases of the change process	Nimrod Vered
❑ Change approvals are documented in a ticketing/tracking system	Nimrod Vered
❑ An up-to-date list is maintained of changes implemented during a specified period of time	Nimrod Vered
❑ Emergency changes are flagged and documented	Nimrod Vered

Deployment Controls

Once the product is tested, it is deployed in the production environment.

Key Security Controls	Responsible Party
❑ Maintain an up-to-date version of the deployment checklist	Nimrod Vered
❑ Access to deploy code to the production environment is limited to only a small set of senior engineers	Nimrod Vered
❑ Define the controls in place to restrict changes to production	Nimrod Vered
❑ A defined process exists for reverting code back to a previous version	Nimrod Vered
❑ A post-implementation review is conducted after a change is pushed to production	Nimrod Vered

Availability

The CTO must monitor the capacity demands of Uplevel systems and make projections of future capacity requirements so that adequate power and data storage requirements can be fulfilled. Utilization of key system resources must be monitored so that additional capacity can be brought on line when required.

Increases in Uplevel business activities and staffing levels must also be monitored to allow for extra facilities which may be required e.g. number of available workstations etc.

Uplevel shall implement and maintain appropriate electronic mechanisms to corroborate that data has not been altered or destroyed in an unauthorized manner.

Uplevel shall maintain and monitor a SLA for its products. The Website shall host the Terms of Service, Privacy Policy, and SLA.

Key Security Controls	Responsible Party
❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	Nimrod Vered
❑ System capacity is monitored in accordance with SLAs and KPIs	Nimrod Vered
❑ System capacity and scaling decisions are communicated to engineering and members of management	Nimrod Vered
❑ Be prepared to describe how system expansion and scaling is forecasted	Nimrod Vered
❑ Load testing is conducted and documented when appropriate	Nimrod Vered
❑ Critical components have been identified and assigned a minimum level of redundancy	Nimrod Vered
❑ Define person in charge of system capacity planning	Nimrod Vered

Incident Reporting

UPLEVEL is responsible for the security and integrity of all data it holds. UPLEVEL must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to UPLEVEL' assets and reputation is prevented and/or minimized. There are many types of incidents which could affect security.

It is the responsibility for all system users to formally report all security incidents, perceived incidents, or violations of the security policy immediately to their immediate supervisor, Security Officer, or any member of the Security Review Team.

UPLEVEL has developed, and maintains a separate, standalone Incident Management Policy. Please refer to this document for the controls referenced.

Key Security Controls	Responsible Party
❑ There is an Incident Management Response Policy and Procedures	Albert Strong
❑ Our incident response and management policy has been reviewed and updated within the last year	Albert Strong
❑ An owner is assigned to the incident response policy	Albert Strong

❑ A process is defined on how employees report incidents internally	Albert Strong
❑ Employees are formally trained on how to recognize an incident and how to report it during the on-boarding process	Albert Strong
❑ All incidents are logged in a centralized ticketing system	Albert Strong
❑ Incidents are classified by their urgency and/or importance and resolved in a timely manner	Albert Strong

Breach Reporting

Security breaches shall be promptly investigated. If criminal action is suspected, the UPLEVEL Security Officer shall contact the management team and appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

UPLEVEL has developed, and maintains a separate, standalone Breach Notification Policy. Please refer to this document for the controls referenced.

Key Security Controls	Responsible Party
❑ A formal breach notification policy is created	Albert Strong

Customer Notification of Change, Status, or Incident

Good communication practices are a key part of building customer trust. Customer trust is especially important for retaining repeat business. Showing integrity when dealing with customer data goes a long way towards building that trust.

Uplevel makes its customers aware of how we value their privacy, and how our internal policies protect them and their information.

Key Security Controls	Responsible Party
❑ The availability of the production website and web app is monitored 24/7/365	Nimrod Vered
❑ Customers are notified in the event of a planned or unplanned downtime	Albert Strong
❑ Customers are notified of application changes and releases that impact the security of data	Albert Strong

❑ Customers have the ability to report software failures, incidents, problems, or complaints.	Albert Strong
❑ A ticket tracking system is used for managing customer issues	Albert Strong
❑ Employees are aware of service level agreements and trained on how to prioritize the resolution of customer issues	Albert Strong

Business Continuity/Disaster Recovery

Uplevel has developed, and maintains a separate, standalone Business Continuity Plan and Disaster Recovery Plan. Please refer to these documents for the controls referenced.

Key Security Controls	Responsible Party
❑ Systems are hosted in a cloud or hosting environment with environmental controls such as a cooling system, generators, redundant communications, smoke detectors, and dry pipe sprinklers	Albert Strong
❑ All third party cloud vendors have a Disaster Recovery Plan	Albert Strong
❑ Maintain an up-to-date Business Continuity Plan	Albert Strong
❑ Maintain documentation describing backup scope and schedule	Albert Strong
❑ Maintain an up-to-date Disaster Recovery Plan	Albert Strong
❑ A list and contact information off all BCDR and data restoration staff is maintained (often part of BCDR plan)	Albert Strong
❑ BCDR tests and/or walk-throughs occur at least annually	Albert Strong
❑ Emergency notification systems are tested at least annually	Albert Strong
❑ Evidence each BCDR test or walk-though is maintained	Albert Strong

Recovery Testing

Full documentation of the recovery procedure must be created and stored. Regular restores of information from backup media must be carried out and tested to ensure the reliability of the backup media and restore process.

Backed up and redundant data systems shall be tested/verified to be operating correctly on an annual basis. To the extent such testing indicates need for improvement in backup procedures, the Security Officer shall identify and implement such improvements in a timely manner.

Retention periods for information and data must be defined and applied to the backup schedule planning. Long term backup and restore solutions need to be identified and applied wherever necessary.

Key Security Controls

- ❑ Backup and restoration process is tested at least annually
- ❑ The data restoration process is defined in a checklist or procedure
- ❑ The data restoration process is available and communicated to all relevant staff

Vendor Management

Definition of Vendor Management

Vendor management is the process that empowers an organization to take appropriate measures for controlling cost, reducing potential risks related to vendors, ensuring excellent service deliverability and deriving value from vendors in the long-run. This includes researching about the best suitable vendors, sourcing and obtaining pricing information, gauging the quality of work, managing relationships in case of multiple vendors, evaluating performance by setting organizational standards, and ensuring that the payments are always made on time.

Benefits of Vendor Management

(1) Better Selection

(2) Better Contract Management

In a multi-vendor scenario, lack of vendor management system elevates the issue of managing contracts, documentation and other vital information in your organization.

(3) Better Performance Management

An integrated view of the performance of all the vendors can be achieved through the implementation of a vendor management system.

(4) Better Vendor Relationship

(5) Better Value

Vendor Management – Risks

(1) Vendor Compliance Risk

(2) Vendor Reputation Risk

(3) Lack of Visibility

(4) Vendor Data Storage

(5) Vendor Payment Risk

Vendor Management Process

(1) Identification and Establishment of Business Goals

Before the vendor management process starts Uplevel will identify and establish business goals that necessitate vendor involvement.

(2) Establishment of a Vendor Management Team

The next step is the foundation of a dedicated vendor management team. This centralized team should be skilled in identifying business goals and KPIs for vendor management, selecting relevant vendors, negotiating the contracting process, periodically assessing the performance of the vendors and tracking all transactions activities.

This team is crucial as they will act as an intermediary between the business units and the vendors and ensure collaboration between the two.

(3) Creation of a Database for all Vendor-related Information

After the business goals are clear and the vendor management team is up and running, the next step should be to build an updated and categorized database of all relevant vendors and vendor-related information.

(4) Identification of the Selection Criteria for Vendors

(5) Evaluation and Selection of Vendors

(6) Developing Contracts and Finalizing Vendors

Vendor Review Procedures

Access to Uplevel computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Uplevel Information Security Policy have been reviewed and considered.
- Policies and standards established in the Uplevel information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform his or her contractual obligations.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.

- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- A formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.
- Non-standard disclosures of sensitive or confidential information to 3rd parties must be approved by the Security Officer or management team members.
- In certain circumstances, a Business Associate Agreement may be required before significant amounts of disclosure to a 3rd party.
- Changes to the amount and type of sensitive or confidential information disclosed to a 3rd party requires the re-authorization by the Security Officer or management team members.

Vendor Communication and Resolution Protocols for Service or Product Issues

As part of identifying all project stakeholders, the project manager will communicate with each stakeholder in order to determine their preferred frequency and method of communication.

In addition to identifying communication preferences, stakeholder communication requirements must identify the project's communication channels and ensure that stakeholders have access to these channels.

Once all stakeholders have been identified and communication requirements are established, the project team will maintain this information in the project's Stakeholder Register and use this, along with the project communication matrix as the basis for all communications.

Vendor Termination Procedures for Poor Performance.

1. document the problems
2. check the contract for responsibilities
3. give written, verifiable notice to the vendor
4. give a written, verifiable opportunity to cure the problem
5. give a written verifiable final compliance date

Vendor Issue resolution and Exception Handling Procedures

In the event a vendor present issues or concerns, the following steps will be employed:

1. Identifying the problem
2. Define the present situation
3. Emplace temporary corrective measures

4. Determine the source of the problem
5. Propose effective solutions
6. Establish an action plan
7. Evaluate the outcomes

Key Security Controls	Responsible Party
❑ Confidentiality agreements are in place for all third party vendors with access to sensitive and confidential data	Albert Strong
❑ Data center service providers are required to sign confidentiality agreements	Albert Strong
❑ SOC 2, or other attestation reports are reviewed from all critical service providers annually	Albert Strong
❑ Document how you monitor all critical service providers for service delivery and compliance	Albert Strong
❑ All new vendors are subject to due diligence and vendor risk assessments	Albert Strong
❑ Vendor agreements are modified as a result of changes to confidentiality practices	Albert Strong
❑ Document the vendor due diligence and risk assessment process	Albert Strong

Data Management

All Uplevel information has a value to the organization, however not all of the information has an equal value or requires the same level of protection. Being able to identify the value of information assets is key to understanding the level of security that they require.

Once the appropriate level of security is identified the appropriate control can be implemented to prevent loss, damage or compromise of the asset, disruption of business activities, and prevention of the compromise or theft of information and information processing facilities. Incorrect classification of assets may result in inadequate or incorrect controls being implemented to protect them.

Information Classification

All information assets will be classified into one of three categories. The information asset must be appropriately labelled to ensure that its classification is readily identifiable.

All information must be categorized using either ‘PUBLIC’, ‘CONFIDENTIAL’ or ‘RESTRICTED’. Any information that is not specifically marked as being ‘RESTRICTED’ or ‘CONFIDENTIAL’ will be deemed to be ‘PUBLIC’. Therefore, the document owner responsible for processing or handling a document, particularly if consideration is being given as to whether a document should be disclosed, MUST consider the content of the document in determining how that document should be processed and not rely on its classification under this policy.

Where information is grouped together, the highest classification shall be applied to all information in the group.

All customer data has been classified as restricted and is subject to the highest level of control.

All Uplevel emails will be classed as ‘CONFIDENTIAL’. The status may be changed to ‘PUBLIC’ or ‘RESTRICTED’ by the user.

Key Security Controls	Responsible Party
Where information is grouped together, the highest classification shall be applied to all information in the group.	Nimrod Vered
All customer data has been classified as restricted and is subject to the highest level of control.	Nimrod Vered
Allcompany emails will be classed as ‘CONFIDENTIAL’. The status may be changed to ‘PUBLIC’ or ‘RESTRICTED’ by the user.	Nimrod Vered
❑ All databases and file storage systems have backups and redundancies in place	Nimrod Vered
❑ Backups are stored offline or in remote site	Nimrod Vered
❑ Backups occur in an automated fashion	Nimrod Vered
❑ Backups occur at least daily	Nimrod Vered
❑ Backups are protected with the same or greater control than production	Nimrod Vered
❑ Backups are encrypted at rest	Nimrod Vered
❑ Backup processes are monitored for failure; failure results in an incident ticket	Nimrod Vered

Data Retention

Backup and Recovery Policy

1. Purpose, scope, and users

The purpose of this policy is to ensure that backup copies are created at defined intervals and regularly tested.

This document applies to the entire Information Security Management System (ISMS) scope, and to all personal data processing activities.

2. Introduction

The Uplevel corporate backup and recovery policy defines the objectives, accountability, and application of backup and recovery of data held in the technology environment of all Uplevel departments.

3. Goals

a. Define and apply a clear backup and restore standard for all corporate information systems.

b. Define backup and recovery standards per data prioritization.

c. Prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.

d. Permit timely restoration of information and business processes, should such events occur.

e. Manage secure backup and restoration processes and the media employed in the process.

f. Set the retention periods of information contained within system level backups designed for recoverability and provide appoint-in-time snapshot of information as it existed during the time-period defined by system backup policies.

4. Policy applicability

List of services and controls where policy applies:

a. Corporate file services:
   i. Uplevel's sensitive/confidential corporate data
   ii. Uplevel's sensitive/confidential customer data

b. Corporate source control services:
   i. Uplevel's intellectual property data

c. Corporate configuration files:
   i. Network device configuration files (corporate firewall, managed switches, routers)

d. Corporate internal services:
   i. Critical services configurations
   ii. Critical resources OS system Uplevels

e. Customers' production applications:
   i. Uplevel's hosted application production deployments serving customers' needs and holding customer's data

5. Principles

The following principles direct this policy:

a. Performing proper backup, storage, and handling of data is necessary to achieve company objectives.

b. All authorized staff must accurately follow the policy and protect the availability, confidentiality, and integrity of data.

6. Policy

a. Data must be protected by regular backups. The Chief Technology Officer must perform backups for internal company data, customers data, and production environment configuration settings.

b. Exceptions to the standard process must be approved by the CISO.

c. All backup data must be stored encrypted with AES-256 symmetric encryption algorithm.

d. Backup copies must be stored in an environmentally-protected and access-controlled secure location offsite from the location of the originating asset.

e. Stored copies must be stored with a short description that includes the following information:

i. Backup date / Resource name / type of backup method (Full/Incremental)

Backup Frequency Schedules

Backing up internally-hosted corporate information systems. The department should maintain the following backup schedule:

Google Drive file shares: Weekly Full backup

- Daily Incremental backup

Source code control:

- Weekly Full backup

Daily Incremental backup

- Configuration files:
- Monthly Full backup

Relevant backup initiated by configuration changes.

- Architecture configuration (backed up by Terra Form or equivalent?
- Internal services and data (license server, etc.):
    - o Weekly Full backup
    - o Daily Incremental backup

Backing up all Customer production environments. DevOps Team should maintain the following backup schedule:

- CORE Production
    - o Backed up via AWS RDS's Automated Backups
    - o Backup retention period 31 days
    - o Amazon RDS automated backup provides an ability to restore to any point in time during your backup retention period up to 5 minutes ago.

Employees

All Uplevel employees are responsible for storing corporate data in the cloud (Box) or on network resources approved by the IT Department. DO NOT STORE CORPORATE DATA ON LOCAL MACHINES.

Key Security Controls	Responsible Party
❑ Maintain a documented data retention policy	Nimrod Vered
❑ Data retention policies are clearly communicated to customers	Nimrod Vered
❑ Old backup data is deleted in accordance with a defined schedule	Nimrod Vered

Testing

Backed up and redundant data systems shall be tested/verified to be operating correctly on an annual basis. To the extent such testing indicates need for improvement in backup procedures, the Security Officer shall identify and implement such improvements in a timely manner.

Retention periods for information and data must be defined and applied to the backup schedule planning. Long term backup and restore solutions need to be identified and applied wherever necessary.

Key Security Controls	Responsible Party
❑ Backup and restoration process is tested at least annually	Nimrod Vered
❑ The data restoration process is defined in a checklist or procedure	Nimrod Vered
❑ The data restoration process is available and communicated to all relevant staff	Nimrod Vered

Data Disposal

Overview

All employees, clients, vendors and contractors have a personal responsibility to keep information secure and confidential. This policy aims to prevent unauthorized disclosure of information assets by the controlled disposal and destruction of media storing confidential data.

Policy

All customer data should be disposed of when it is no longer necessary for business use, provided that the disposal does not conflict with our data retention policies, our customers data retention policies, a court order, or any of our regulatory obligations.

All employees, clients, vendors and contractors are instructed to not use the following media to store confidential information.

- paper-based media
- USB Drives or External Backup programs
- CD ROM drives.

All cloud based storage media being decommissioned should be sanitized when it is no longer necessary, provided that there is a backup of customer data on production systems to comply with our customers data retention and contractual obligations.

Laptop based storage media may not be donated or sold. All laptop based storage media should be sanitized prior to transfer of ownership to a co-worker or prior to destruction.

Scope

The following table displays the forms of storage media currently in use.

Media Type	Location	Data Storage Mechanism	Removal Methods
Hard Disk Drives Destruction	Laptop	Non-volatile Magnetic	Clearing,
Solid State Drives	Laptop Solid State	Clearing, Destruction	
Amazon S3	Cloud	Non-volatile magnetic	(DoD) 5220.22-M
Amazon EFS	Cloud	Solid state	(DoD) 5220.22-M
Amazon EBS	Cloud	Solid state	(DoD) 5220.22-M

Removal Classifications

A) Clearing

If comprehensive data removal from the media is not required, then non-specialist staff or contractors may carry out clearing. Typical clearing programs use sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs. To ensure that historical data is thoroughly removed it is advisable to make as many passes as is practicable.

B) Purging

Purging is a more advanced level of sanitization that renders media unreadable even through an advanced laboratory. After removal of media from its current security context there must be sufficient care taken to ensure that data is irretrievable. If purging of the media is required, a minimum of seven passes qualifies as a purging process.

C) Destroying

Destroying renders media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting.

Media Destruction Techniques

Storage Media, which is being decommissioned, will be passed to a specialist contractor for secure disposal.

A) Hard Disk Destruction

Degaussing is a simple method that permanently destroys all data and disables the drive. Degaussing uses a high-powered magnetic field that permanently destroys data on the platters. The recommended specification for data destruction is the SEAP 8500 Type II standard used for classified government material.

C**) Solid-State Devices**

Solid-state devices normally require the complete physical destruction of the device to ensure that any recovery of data is impossible. Incineration will melt SD cards. Devices such as USB thumb drives should be physically destroyed using brute force methods. As long as appropriate safety methods are in use, non-specialist staff can destroy these devices.

D) Cloud Based(AWS) Devices

“When AWS determines that media has reached the end of its useful life, or it experiences a hardware fault, AWS follows the techniques detailed in Department of Defense (DoD) 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST SP 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process.” P.39 AWS Security Best Practices White paper

Data Removal and Destruction Management

Once a specialist company or contractor has processed the media, there should be a procedure for verification of data removal. It is important to maintain an effective method of managing the process of data destruction. This ensures that all media requiring cleaning or destruction is correctly organized and properly audited. Tracking of hard disk serial numbers should be used a bare minimum for individual component tracking.

Key Security Controls	Responsible Party
❏ Sensitive information is systematically erased when no longer required	Nimrod Vered
❏ Sensitive paper records are destroyed when no longer required	Nimrod Vered
❏ Data destruction processes are reviewed annually	Nimrod Vered

Procedure for Updating Controls

The Security Controls as described herein must be observed, maintained and documented throughout the year. A “Control Calendar” is provided below with monthly reminders of which controls must be reviewed for that month, be they monthly, quarterly, semi-annually, or annual.

A column is provided for the review to be documented.

The review shall be undertaken by the CEO, CTO and CISO in a monthly meeting. Minutes of the meeting will be recorded documenting the review.

Control Calendar

January			**Evidence of Review**
	Annual	❑ Maintain up-to-date bios for all key executives	
	Annual	❑ Maintain an up-to-date org chart for all key executives	
	Annual	❑ An Senior Officer is named as Chief Information Security Officer	
	Annual	❑ The Security Officer has a documented job description	
	Annual	❑ Establish a Security Review Board	
	Annual	❑ Members of the Security Review Board are appointed by the Security Officer	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
	Quarterly	❑ The Board of Directors provides management oversight	
	Quarterly	❑ The SRB will meet at least Quarterly to discuss security issues	
	Quarterly	❑ Control self-assessments are performed on a quarterly basis by process owners and results are communicated to management	
	Quarterly	❑ Meeting minutes and/or agendas are kept when reviewing operation metrics	
	Quarterly	❑ Load testing is conducted and documented when appropriate	
	Semi-Annual	Post Implementation Review – Complete review of SDLC process for a major release	
February			**Evidence of Review**

	Annual	❑ Review and update job descriptions annually	
	Annual	❑ Ensure key responsibilities are in each job description	
	Annual	❑ Ensure security responsibilities are in each job description	
	Annual	❑ Job description management process should have an owner	
	Annual	❑ Workplace Conduct Standard Policies are maintained and updated annually.	
	Annual	❑ New employees are required to sign a confidentiality agreement	
	Annual	❑ Maintain and up-to-date employee handbook	
	Annual	❑ Employee handbook and code of ethics is acknowledged annually	
	Annual	❑ Annual performance reviews are conducted for all employees	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
			Evidence of Review
March			
	Annual	❑ Security awareness training for all employees is renewed annually	
	Annual	❑ Security awareness training is tracked; records are kept	
	Annual	❑ Maintain up to date security awareness documentation	
	Annual	❑ Maintain an up-to-date version of the company's SLA.	
	Annual	❑ A privacy notice or policy is posted on the company website	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
			Evidence of Review

April	Annual	❑ Information Security Policy is reviewed and updated annually	
	Annual	❑ Data and asset inventories are updated annually	
	Annual	❑ Maintain an up-to-date version of the component/asset inventory	
	Annual	❑ A data inventory is created listing and describing key classes of data managed	
	Annual	❑ Maintain an up-to-date version of the data inventory	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
	Quarterly	❑ The Board of Directors provides management oversight	
	Quarterly	❑ The SRB will meet at least Quarterly to discuss security issues	
	Quarterly	❑ Control self-assessments are performed on a quarterly basis by process owners and results are communicated to management	
	Quarterly	❑ Meeting minutes and/or agendas are kept when reviewing operation metrics	
	Quarterly	❑ Load testing is conducted and documented when appropriate	
			Evidence of Review
May	Annual	❑ A formal risk assessment and management process is documented	
	Annual	❑ Maintain an up-to-date version of the company’s risk assessment policy and procedure	
	Annual	❑ Maintain an up-to-date version of the company’s Risk Register	
	Annual	❑ Security topics and risk are regularly discussed in management meetings	
	Annual	❑ Meeting agenda/notes document risks that are discussed	
	Annual	❑ Formal risk assessment is conducted annually using the Risk Register	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	

	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
			Evidence of Review
June	Annual	❑ Control-self-assessment, reviews, and/or internal audits are performed quarterly	
	Annual	❑ External penetration testing/vulnerability assessments are conducted annually	
	Annual	❑ Our organization has general liability insurance/cyber insurance	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
	Semi	❑ Maintain up to date network and/or system architecture diagram.	
	Semi	❑ Physical and logical architectural diagrams are updated annually	
	Semi	❑ Log and alerting processes are reviewed on a semi-annual basis	
	Semi	❑ Admin, application, and security event logs are included in the review	
	Semi	❑ Production environment configurations/defaults reviews are performed semi-annually	
	Semi	❑ All engineers are made aware of the OWASP and secure development coding practices and developers, implementation specialist, system operation specialist are required to undergo security training on a regular basis	
	Semi	❑ Roles and access rights are reviewed on all key production/operational systems, and physical offices semi-annually	
			Evidence of Review
July	Annual	❑ A SOC 2 internal audit by a Certified Public Accounting firm will performs control assessments on an annual basis and communicates results to management	

	Annual	❑ Production systems and servers have been hardened to ensure an appropriate level of security against a documented standard	
	Annual	❑ Scans are conducted on production systems and servers to validate the hardening is successful	
	Annual	❑ Maintain an up-to-date list of what practices/standards that are used in the hardening process	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
	Quarterly	❑ The Board of Directors provides management oversight	
	Quarterly	❑ The SRB will meet at least Quarterly to discuss security issues	
	Quarterly	❑ Control self-assessments are performed on a quarterly basis by process owners and results are communicated to management	
	Quarterly	❑ Meeting minutes and/or agendas are kept when reviewing operation metrics	
	Quarterly	❑ Load testing is conducted and documented when appropriate	
	Semi-Annual	Post Implementation Review – Complete review of SDLC process for a major release	
			Evidence of Review
August	Annual	❑ Maintain a list of all the individuals who have the responsibility of creating and managing accounts	
	Annual	❑ All user login IDs are audited at least twice yearly	
	Annual	❑ All workstations/laptop drives are encrypted	
	Annual	❑ Maintain an up-to-date version of the deployment checklist	
	Annual	❑ All workstations and laptops have malware protection installed	
	Annual	❑ Be prepared to describe how system expansion and scaling is forecasted	

	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
			Evidence of Review
September	Annual	❑ All employees and contractors have read and signed the Workstation and Laptop Security Policy	Mgt meeting 9/23/2020; See minutes
	Annual	❑ An email system is utilized with built-in spam and malware detection	Mgt meeting 9/23/2020; See minutes
	Annual	❑ Installation of software on workstations or laptops is prohibited except to only approved applications	Mgt meeting 9/23/2020; See minutes
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	Mgt meeting 9/23/2020; See minutes
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	Mgt meeting 9/23/2020; See minutes
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	Mgt meeting 9/23/2020; See minutes
			Evidence of Review
October	Annual	❑ Our incident response and management policy has been reviewed and updated within the last year	Reviewed 10/28/2020 See mgt mtg minutes
	Annual	❑ An owner is assigned to the incident response policy	Reviewed 10/28/2020 See mgt mtg minutes
	Annual	❑ Maintain an up-to-date Business Continuity Plan	Reviewed 10/28/2020 See mgt mtg minutes
	Annual	❑ Maintain an up-to-date Disaster Recovery Plan	Reviewed 10/28/2020 See mgt mtg minutes
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	Reviewed 10/28/2020 See mgt mtg minutes
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	Reviewed 10/28/2020 See mgt mtg minutes
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	Reviewed 10/28/2020 See mgt mtg minutes
	Quarterly	❑ The Board of Directors provides management oversight	Reviewed 10/28/2020 See mgt mtg minutes

	Quarterly	❑ The SRB will meet at least Quarterly to discuss security issues	Reviewed 10/28/2020 See mgt mtg minutes
	Quarterly	❑ Control self-assessments are performed on a quarterly basis by process owners and results are communicated to management	Reviewed 10/28/2020 See mgt mtg minutes
	Quarterly	❑ Meeting minutes and/or agendas are kept when reviewing operation metrics	Reviewed 10/28/2020 See mgt mtg minutes
	Quarterly	❑ Load testing is conducted and documented when appropriate	Reviewed 10/28/2020 See mgt mtg minutes
			Evidence of Review
November	Annual	❑ Backup and restoration process is tested at least annually	
	Annual	❑ The data restoration process is available and communicated to all relevant staff	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	
			Evidence of Review
December	Annual	❑ Confidentiality agreements are in place for all third party vendors with access to sensitive and confidential data	
	Annual	❑ Data center service providers are required to sign confidentiality agreements	
	Annual	❑ SOC 2, or other attestation reports are reviewed from all critical service providers annually	
	Annual	❑ All new vendors are subject to due diligence and vendor risk assessments	
	Annual	❑ Old backup data is deleted in accordance with a defined schedule	
	Annual	❑ Data destruction processes are reviewed annually	
	Monthly	❑ Internal/External application and network layer vulnerability scans are performed on a monthly basis	
	Monthly	❑ System capacity is monitored on a continuous basis (CPU, memory, storage, and bandwidth)	
	Monthly	❑ The availability of the production website and web app is monitored 24/7/365	

	Semi	❑ Maintain up to date network and/or system architecture diagram.	
	Semi	❑ Physical and logical architectural diagrams are updated annually	
	Semi	❑ Log and alerting processes are reviewed on a semi-annual basis	
	Semi	❑ Admin, application, and security event logs are included in the review	
	Semi	❑ Production environment configurations/defaults reviews are performed semi-annually	
	Semi	❑ All engineers are made aware of the OWASP and secure development coding practices and developers, implementation specialist, system operation specialist are required to undergo security training on a regular basis	
	Semi	❑ Roles and access rights are reviewed on all key production/operational systems, and physical offices semi-annually	

Version History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version			
2.0	Final Version	4/21/2020		Joe Levy
3.0	Major Updates	7/03/2020		Joe Levy
4.0	Major Updates	7/14/2020	7/14/2020	Joe Levy
5.0	Major Updates	8/24/2020	8/24/2020	Joe Levy
6.0	Final Changes	9/04/2020	9/04/2020	Joe Levy
7.0	September Control Reviews	9/26/2020	9/26/2020	Joe Levy
8.0	October Control Reviews	10/28/2020	10/28/2020	Joe Levy
9.0	Review	12/28/2021	12/28/2021	Albert Strong

Approved by:

Job Title	Name
Chief Executive Officer	Joe levy
Chief Technology Officer	Nimrod Vered
Chief Information Security Officer	Albert Strong

Acknowledgement of Receipt of Information Security Policy

Employee/Contractor:

I acknowledge that I have received a copy of the Uplevel Information Security Policy. I have read and agree to abide by all policies and procedures contained therein.

By: ____ Date: _____________________