Security Posture

1 November 2022

Version v2.3

Table of Contents

1 Version History

Date of Revision	Changes
20 December 2020	V1 - Initial version
8 March 2021	V2 - Revised to reflect changes to platform architecture (Auth0) and operational improvements
10 May 2021	V2.1 – minor revisions to reflect improved operations (dependabot) and Australian operations.
12 August 2021	V2.3 – minor adjustment to backups – added in the use of Okta SSO

2 Introduction

Trust is the foundation of our relationship with property development businesses around the world. In turn, that trust needs to extend to the thousands of users that we support in their working lives every single day. We value the confidence that our customers put in us and take the responsibility of protecting their information and information of their users, incredibly seriously.

To be worthy of your trust, we have built and will continue to grow LandTech with an emphasis on security, compliance and privacy.

To help our customers understand how we operate, this whitepaper describes LandTech's application architecture, and related security aspects of our SaaS applications as well as details on our data centre provider, Amazon Web Services. This guide includes network firewalls, data privacy, disaster recovery, and auditing and compliance processes and procedures.

As part of our planning and consideration for the delivery of secure services, we have chosen Amazon Web Services (AWS) as our provider of data centre capability.

3 AWS Physical and Operational Security

3.1 AWS Data Centres

Site Selection

Prior to choosing a location, AWS performs initial environmental and geographic assessments. Data centre locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. AWS Availability Zones are built to be independent and physically separated from one another.

Redundancy

Data centres are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data centre failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Availability

AWS has identified critical system components required to maintain availability and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, LandTech can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

Capacity Planning

AWS continuously monitors service usage to deploy infrastructure to support availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

3.2 Business Continuity & Disaster Recovery

Business Continuity Plan

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

Pandemic Response

AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

3.3 Physical Access

Employee Data Centre Access

AWS provides physical data centre access only to approved employees. All employees who need data centre access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Third Party Data Centre Access

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

3.4 Monitoring & Logging

Data Centre Access Review

Access to data centres is regularly reviewed. Access is automatically revoked when an employee's record is terminated in Amazon's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

Data Centre Access Logs

Physical access to AWS data centres is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

Data Centre Access Monitoring

AWS monitors its data centres using global Security Operations Centres, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data centre access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analysing, and dispatching responses.

3.5 Surveillance & Detection

CCTV

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

Data Centre Entry Points

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centres. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

Intrusion Detection

Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are

immediately dispatched to 24/7 AWS Security Operations Centres for immediate logging, analysis, and response.

3.6 Device Management

Asset Management

AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

Media Destruction

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

3.7 Operational Support Systems

Power

AWS data centre electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centres are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Climate and Temperature

AWS data centres use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Fire Detection and suppression

AWS data centres are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

Leakage Detection

In order to detect the presence of water leaks, AWS equips data centres with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

3.8 Infrastructure Maintenance

Equipment Maintenance

AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centres. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Environment Management

AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

3.9 Governance & Risk

Ongoing data centre risk management

The AWS Security Operations Centre performs regular threat and vulnerability reviews of data centres. Ongoing assessment and mitigation of potential vulnerabilities is performed through data centre risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

Third party security attestation

Third-party testing of AWS data centres, as documented in third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data centre, test electronic access control devices, and examine data centre equipment.

3.10 Certifications

AWS maintains SSAE16/SOC1 and SOC2 annual reports and performs annual audits to maintain these certifications. AWS also has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2014, and ISO/IEC 9001:2015. AWS services that are covered under the certifications are listed below.

4 LandTech Business Security

LandTech maintains stringent physical security at its offices. Reference checks are mandatory for all employees and contractors. Employees and contractors are required to sign a Proprietary Information Agreement as a condition of employment. Each person with authorized access is provided an electronic key to gain entry and move within facilities.

Access passwords are revoked every 30 days as part of comprehensive user ID revalidation. There is a formal procedure to add, delete, and modify user accounts and access, assign roles, and perform audit compliance.

The LandTech people team provides alerts to Corporate IT and applicable Operations personnel when an employee is terminated. Corporate IT then disables network/e-mail/application access as per the people teams alert's listed time frame (immediate or scheduled). Privileged user accounts are controlled and reviewed quarterly.

Executive Management has issued, approved, and supported a set of policies, procedures, and guidelines to ensure security across the entire business. These policies include an Information Sensitivity Policy, Data Handling Policy, and LandTech Secure Coding Guidelines. All personnel with access to customer data are required to certify that they have read and will comply with the policies.

PCs, laptops, and servers are protected against viruses and malware by anti-virus software (Crowdstrike Falcon) that receives automatic updates and daily virus definition updates.

Recently LandTech have began using SSO Technology (Okta SSO) to further strengthen its Security Policies. Single Sign-On (SSO) is a technology which combines several different application login screens into one. With SSO, a user only has to enter their login credentials (username, password, etc.) one time on a single page, to access all of their SaaS applications.

5 Application Architecture

5.1 Software Development Process

LandTech's software development process follows the OWASP (Open Web Application Security Project) standards for building secure applications, including internal security reviews. Our software development cycle includes mandatory stringent code reviews, integration and regression testing, and full internal and external security testing to check for vulnerabilities. Results are shared with the development team and issues are resolved prior to every release. Security testing includes pre-release and post-release validation.

Weekly application vulnerability scans are also conducted to ensure software components remain secure and no vulnerabilities are introduced. All third party and open source components used in LandTech services are selected based on their stability and support and are included in the SDLC (Systems Development Life Cycle) and in the scope of the vulnerability scans.

All components of the software platform are kept current with regular release updates and patches as necessary. LandTech's devops team reviews the appropriate patches and then creates a rollout plan consisting of planning, deployment, and testing. We use technologies such as GitHub's Dependabot, which automatically creates Pull Requests (for manual review), when security advisories are issued for Python and Javascript dependencies.

New application features are designed to be forward and backward compatible, and when deployed, not to affect customer instances (for example, customers must positively enable new features when they become available). New features are outlined in product documentation, and our customer success team reviews features with customers prior to release.

5.2 Software Architecture

Customers gain access to LandTech's SaaS applications through our user facing web applications (such as LandInsight, LandFund and LandEnhance) or via LandTech's family of APIs (Application Programming Interface).

5.3 Authentication and Access Controls

LandTech applications are accessible via current web browsers such as Safari, Google Chrome and Firefox. Our API is accessible via any client capable of communicating with APIs over the HTTP transport. Authentication services are provided by Auth0, a world leader in authentication and identity management. API user actions are tracked in audit logs. Session timeouts automatically log an idle user out of the applications.

5.4 Multi Factor Authentication

Access to all production resources (i.e AWS, Github, MailChimp, CircleCI, MongoDB, Postgres etc) require two factor authentication, which is initially administered by our IT Operations team.

5.5 Network Security

LandTech implements AWS best practices in the design and configuration of its network. All network traffic is encrypted using TLS 1.2.

5.6 Network Architecture

Network access to and from LandTech applications is controlled by dedicated firewall devices, Intrusion Detection/Prevention Systems (IDS/IPS), access control lists, and load balancing. Employee access to LandTech production servers requires AWS access with multi-factor authentication and is regularly audited. Distributed Denial of Service (DDoS) mitigation services are used to protect servers and prevent impact on the service to customers. The network that hosts

customer data and manages customer transactions is completely separate from LandTech's corporate network.

Firewalls – provide traffic filtering and intrusion prevention services. The clustering technology provides sub-second failover in the event of a hardware problem.

Intrusion Detection and Prevention – Network IDS/IPS functions are handled by enhanced firewall modules or dedicated IPS devices.

Two-factor Authentication – Authorised Operations personnel access the production environments using two factor authentication – a user login and password, and SecurID tokens.

5.7 Data Security

LandTech's data security and protection controls focus on employee access to systems that house customer data, regulatory compliance, data encryption, user roles, and data retention/destruction.

Administrative Controls

Data access – Access to customer data is restricted to authorised Customer Support, Operations, and limited Engineering personnel. In all cases, employees have to request access to a Manager that grants access to a specific customer subscription for a limited period of time. Access to SaaS servers is restricted, logged, tracked, and regularly audited.

Data security policies – These include our Customer Data Handling Policy and our Secure Document Destruction Policy. All employees who have access to customer data and/or production systems must attend annual security and data privacy training to ensure compliance with corporate security policies and practices.

Quarterly audits ensure that all access to customer data and production systems by authorized personnel is compliant with all security policies.

Data Encryption, Protection and Destruction

Customer data in transit is encrypted using high grade TLS encryption.

For data protection, LandTech uses effective and efficient storage-based technologies that enable hourly snapshot backups. These can be used within a data centre for quick data recovery. For offsite DR backups, all production data is sent either to another data centre in the same country or to an offsite data storage facility every 24 hours.

If a customer terminates its LandTech subscription, data contained in that subscription is retained within our systems for 30 days and is then securely and irrevocably deleted.

5.8 Data Encryption

LandTech stores customer data in an unencrypted form, at rest.

5.9 Data Storage Location

For European customers, LandTech stores all data within the European Economic Area (EEA). We are currently evaluating AWS storage options and locations, for our upcoming Australian solutions.

5.10 Data Processing

Land Technologies Ltd is registered with the UK Information Commissioners Office (https://ico.org.uk) in the UK. Our registration number is ZA497002.

6 Business Continuity and Disaster Recovery

LandTech's data protection, high availability, and built-in redundancy ensure application availability and protect information from accidental loss or destruction.

6.1 Summary

- AWS data centres have redundant power, fire prevention, network paths, and generators to survive moderate disaster scenarios
- We have backups for all data centres
- All LandTech networking, storage, servers and databases, power and network paths are redundant within a data centre and can sustain hardware failures and failures of individual software components.
- The entire LandTech platform can be rebuilt from scratch, via automation, in less than 4 hours.
- RPO is 24 hours, RTO is 48 hours.

6.2 Backup and Recovery

Our primary data backup strategy leverages the snapshot and data mirroring capabilities provided by the AWS enterprise storage systems. Backups are performed automatically every 24 hours. To satisfy data privacy requirements, backups are never sent across borders in any of the AWS data centres. The integrity of local backups is tested quarterly by restoring the entire LandTech service from selected snapshot copies onto a test system and verifying the data.

6.3 Network and Storage Redundancy

Every component in the SaaS infrastructure is redundant. There are at least two of each hardware component that process the flow and storage of data. All network devices, including firewalls, load balancers, and switches, are fully redundant and highly-available. High availability for Internet connectivity is ensured by multiple connections in each data centre to different ISPs.

6.4 Load Balancing and server clustering

LandTech load-balances at every tier in the infrastructure, from the network to the database servers. Application server clusters are enabled to ensure that servers can fail without interrupting the user experience. Masterless database servers are clustered across all data centres for high tolerance and reliability.

6.5 Disaster Recovery (DR) Plan

LandTech's Disaster Recovery plan incorporates geographic mutual failover between AWS datacentres in Ireland. Service restoration is within commercially reasonable efforts.

6.6 Business Continuity

The SaaS service functions have no direct dependencies on LandTech office facilities. As a remote first employer, LandTech does not have a significant reliance on corporate headquarters-based personnel to perform critical functions.

6.7 Monitoring Services and Security Audits

Monitoring and Incident Reporting

LandTech uses a variety of methods to monitor and enhance application and data security.

Application access logging – All successful and unsuccessful access activities are recorded in the system and in application logs, including organisation, action, and date/time of access. Every data change is logged in the system and in application logs. Application logs are stored tamper-proof for six months.

Software coding methodology – Software development at LandTech includes thorough documentation and disciplined use of a version control process (Github). Every release starts with a detailed design process involving Engineering and Product Management. Once the release plan and dates are finalized, we follow an iterative planning/design/development process with regular demos and feature completion check-off.

QA performs rigorous regression and stage testing, and the automated tooling performs release readiness checks before deployment is allowed to occur. In addition to our development methodology, LandTech has formal processes for software escalation issues and on-demand triages for bug fixes and patches. All development engineers are required to take secure coding training.

Intrusion detection – Intrusion Detection Systems (IDS) are in place at the network perimeter and at critical locations in the server system. For network-based devices, intrusion detection is an event-driven activity triggered either by IDS alerts or by a LandTech request to investigate suspicious activity.

Alerting – Our devops team monitors and alerts customers of suspicious activity, including but not limited to multiple failed authentication attempts, abnormal usage patterns, and large data access/downloads. LandTech has a formal process to notify customers of a verified security breach, theft, or loss of data. This process and policy are part of our commitment to transparency. We respond to High alert (P1) incidents on a 24x7 basis and all incidents are tracked in a case management system (Clubhouse).

Security Audits

LandTech performs the following scheduled tests :

- Vulnerability Testing – We are currently evaluating vulnerability testing solutions, as part of our ongoing security improvement and ISO 27001 continuous enhancement programme.
- Penetration Testing – We undertake penetration testing at least once a year using an external security vendor. A redacted copy of the latest report is available upon request, subject to an NDA being in place.

7.3 Internal Audits

In addition to security audits, LandTech conducts internal audits on:

- Employees and contractors during the hiring process
- Backup media and data
- Application and data access by users

Audit trail logs include all customer browser activity, application logs, and email campaign logs. Logs are stored for 90 days online on application servers, and subsequently for 6 months in archive.

Problem Resolution Management

LandTech’s customer-centric business philosophy and culture is strongly reflected in its superior customer service. Customer issues can be logged 24x7 with customer support, and Production personnel are available 24x7. We offer value-based support programs to meet your requirements.

Email requests are validated against the customer contact information on file. Phone requests are validated against a phone number and positive contact lists if requested.

LandTech operates to a 99.99% service availability plan.

6.8 Apple Device Management / Mobile Device Management

LandTech makes extensive use of Apple laptops and mobile devices. To securely support these devices, and ensure compliance with our various policies, we use Kandji, a modern, cloud-based platform that streamlines tasks for IT administrators, making it easier to quickly and securely manage and deploy Apple devices among LandTech's distributed workforce. Kandji ensures that all devices are kept up to date with the latest software patches, and that users have appropriate privileges, depending upon their role. Onboarding and offboarding of staff is also automated via Kandji.

6.9 Cyber Essentials

LandTech is certified under the UK Cyber Essentials programme, operated by the UK National Cyber Security Centre – our certificate is IASME-CE-010442.

7 Summary

At LandTech, security, integrity, and the availability of our customers' data are our top priorities. We believe this is vital to your business operations and to our own success. We use a multi-layered security approach, involving data privacy, application security, physical and environmental security, network access controls, monitoring and incident reporting, administrative and service availability controls, and regulatory compliance.

LandTech has a perfect track record of zero known security breaches. We host customer data at SSAE16 or ISO 27001 certified datacentres operated by AWS.

LandTech is also ISO 27001 certified.