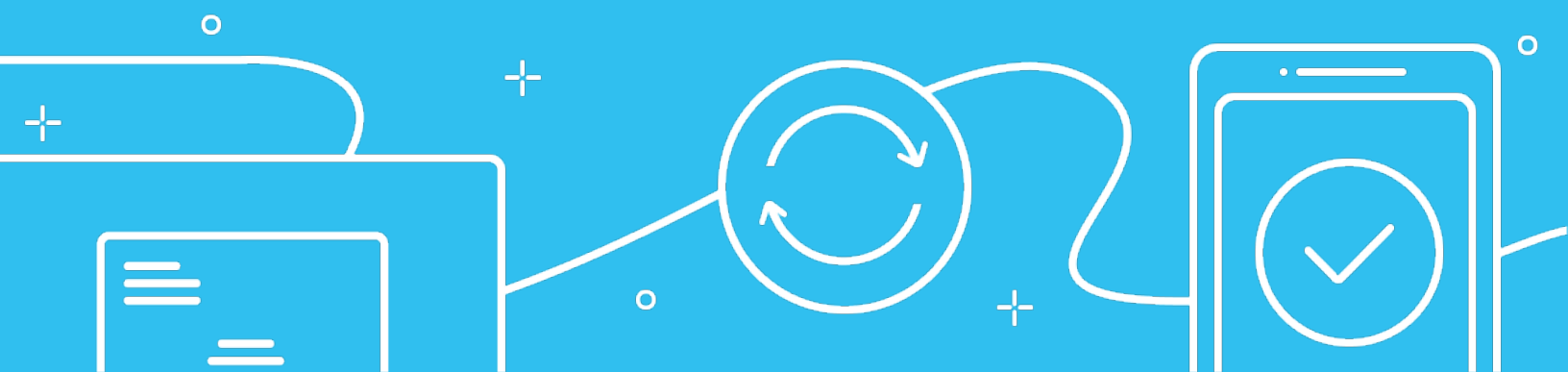
mobile recell

IT Asset Recovery Glossary



4G

Fourth generation of broadband mobile cellular network technology. 4G users get speeds of up to 100Mbps, while 3G only promises speeds of 14Mbps.

5G

Fifth generation of broadband mobile cellular network technology. Designed to greatly increase the speed and responsiveness of wireless networks, users can expect speeds as high as 20 Gbps—more than 200 times faster than 4G broadband.

Apple Business Manager (ABM)

Web-based portal for IT administrators to automate device enrollment, giving organizations a fast, streamlined way to deploy corporate-owned Apple devices and enroll in MDM without having to touch or prepare each device physically.

application programming interface (API)

Software code allowing two software applications to easily and securely exchange data and functionality.

asset recovery as a service (ARaaS)

Full-service IT asset recovery and disposition offering allowing customers to leverage software to monitor the transparent and secure recovery and disposition of assets, with market experts guiding the entire process; eases the IT needs of a company by outsourcing IT asset recovery and resale or recycling.

average sale price (ASP)

Amount of money a specific mobile device model is sold for across different markets and channels.

bring your own device (BYOD)

Enterprise mobility program allowing employees to use their personal IT assets—such as smartphones, tablets, laptops, and wearables—for work-related activities.

buyback

Process in which a technology hardware or service provider offers to purchase a customer's old hardware outright, which can be resold in secondary markets or provide raw materials reused to make new IT assets more environmentally friendly. *See trade-in.*

certificate of data destruction (CODD)

Formal document stating digital media and confidential data have been destroyed beyond recovery for an identifiable, specific IT asset—typically electronics, documents, hard drives, and other data-containing media.

certificate of destruction (COD)

Formal document stating an identifiable, specific IT asset—such as a smartphone, tablet, or laptop—has been destroyed beyond recovery.

certified data erasure

Accredited software-based method of securely overwriting data, completely destroying all electronic data from the IT asset in accordance with NIST 800-88, DoD 5220.22-M, SOC, ADISA, ISO 27001, GDPR, or PCI-DSS guidelines.

compliance report

Automated, software-driven report identifying which end users have not started the return of their corporate-owned IT assets as requested, allowing the enterprise to take action through configurable reminders and notifications.

corporate-liable (CL)

Enterprise mobility program in which an organization provides employees with company-owned IT assets, or the employee purchases the IT assets and is reimbursed under a formal policy. COBO, COPE, and CYOD mobility programs are also Corporate-Liable (CL) programs.

corporate-owned, business-only (COBO)

Enterprise mobility program in which an organization provides employees with business-only mobile devices that only have business-related applications installed and require IT credentials to download other apps; usually interchangeable with corporate-liable (CL).

corporate-owned, personally-enabled (COPE)

Enterprise mobility program in which an organization issues an employee a pre-selected mobile device to use primarily for business purposes.

choose your own device (CYOD)

Enterprise mobility program that allows employees to select a corporate-owned device from a list of pre-approved mobile devices, which are pre-programmed with security applications to safeguard company data while the device is in use and can be used for personal and work-related purposes.

cryptographic erasure (CE)

Data handling and encryption process ensuring an IT asset's data is impossible to decrypt, rendering the data unrecoverable.

customer experience (CX)

Product of interaction between an organization and its customer over time; designed to deliver value to the customer by helping them achieve their business goals.

data breach

Security incident in which confidential, sensitive, or protected data is accessed, stolen, or transmitted without the knowledge or authorization of the system's owner.

data destruction

Software-based method that uses zeros and ones to overwrite data and completely destroy all electronic data residing on an IT asset.

data security

Protection of digital information from unauthorized access, corruption, or theft throughout its entire lifecycle.

Department of Defense (DoD) 5220.22-M Standard

Common data erasure method used by government agencies and organizations for performing data erasure.

Device Enrollment Program (DEP)

Program helping companies to easily deploy and configure Apple devices; replaced by Apple Business Manager (ABM) in December 2019.

device processing

Process all devices must endure at the end of their lifecycle to determine which path the device should take—reallocation in the secondary marketplace, redeployment for reuse, or responsible recycling—to end the device's lifecycle. *See device triage.*

device triage

Process all devices must endure at the end of their lifecycle to determine which path the device should take—reallocation in the secondary marketplace, redeployment for reuse, or responsible recycling—to end the device's lifecycle. *See device processing.*

DevSecOps

Combines aspects of development, security, and operations to ensure software security is integrated at the beginning of and throughout the software development process.

diagnostic functionality testing

Testing process all devices must endure to determine the functionality of various components—audio, cameras, components, connectivity, and display; results of this testing influence the grade assigned to the device post-processing.

employee purchase program

Incentive program providing employees a convenient way to purchase the familiar mobile devices they use for work at the end of the IT asset's lifecycle using payroll deduction or through a direct discount.

encryption

Algorithmic process converting data into a code to prevent unauthorized access.

endpoint

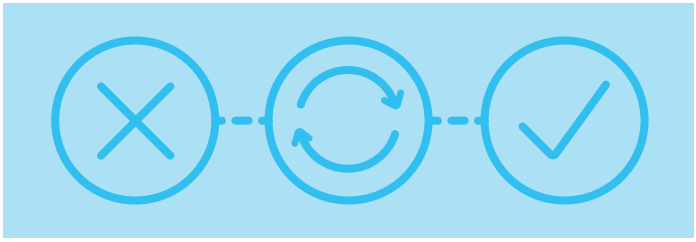
Internet-capable IT asset that sends data to and receives data from its connected network.

endpoint protection

Solution for mobile devices that gives system admins a centralized management dashboard, allowing them to secure all devices connected to their corporate network.

end-user computing (EUC)

End-user access and service support focusing on applications, data, and IT assets.



enrollment status

Status given to each processed device to determine if there are enterprise or end-user locks hindering full functionality of the IT asset.

enterprise mobility

Approach to work in which employees can do their jobs from anywhere using a variety of devices and applications.

enterprise mobility management (EMM)

Software ensuring program and policy compliance by managing mobile devices, content, information, and risks to secure mobility program data, services, and usage. EMM evolved from mobile device management (MDM) as a comprehensive solution protecting more than just a physical device.

environmental impact report

Report showing how an IT asset lifecycle program is creating a sustainable solution—by reselling, reusing, and recycling assets—and saving e-waste materials from landfills.

environmental, social, governance (ESG)

Framework designed to create enterprise value by expanding the organizational objectives to include environmental, social, and governance initiatives.

e-Stewards

End-to-end accountability system to prove e-waste recycling is performed with core objectives of data security, health, and worker safety, responsible export practices, and zero use of prison labor, dumping, or incineration.

e-waste

Discarded electronic devices that are unwanted, not functioning, or at the end of their lifecycle.

General Data Protection Regulation (GDPR)

Legal framework that protects personal information by setting guidelines for the collection and processing of data from European citizens and residents. Although GDPR is established in the EU, the rules and regulations apply to companies in the US, especially those that conduct business with the EU or have European clients.

Global Reporting Initiative (GRI) Standards

Modular system of interconnected standards allowing companies to publicly report the impacts of their activities in a way that is transparent to stakeholders.

Global System for Mobility (GSM)

International telecommunications standard for transmitting voice and data between mobile devices. Mobile devices employing this technology use SIM cards, allowing them to be used on multiple carrier networks.

grade

Assigned classification a device receives post-processing regarding its functionality and cosmetic condition. Industry standards refer to a grading system similar to the educational system to grade devices, where A signifies a device in pristine condition, and where D or F signifies a broken or non-functional device.

human capital management system (HCMS)

Software typically providing tools for talent acquisition, talent management, and talent organization to manage the HR actions aligning with the employee lifecycle—onboarding, performance tracking, compensation, and offboarding.

human resources information system (HRIS)

Software managing most human resources operations for an organization with a focus on people, procedures, and policies.

human resources management system (HRMS)

Software combining systems and processes to ensure the easy management of human resources operations, business processes, and data; includes HR procedures and policies and the employee lifecycle—onboarding, performance tracking, compensation, and offboarding.

identity and access management (IAM)

Software helping securely control access to authentication resources for authorized users only.

international mobile equipment identity (IMEI)

A 15- or 17-digit number uniquely identifying an IT asset.

Internet of Things (IoT)

System of interrelated computing devices that are uniquely identifiable and maintain continuous network connectivity, allowing the connected devices to constantly send and receive data across a network with little or no manual interaction.

ISO (International Organization for Standardization) certification

International standard certifying a management system, manufacturing process, or documentation procedure has all the requirements for standardization and quality assurance. ISO certification ensures consistency, quality, product safety, and compatibility.

ISO 9001:2015

Criteria for a quality management system based on a number of principles, including a strong customer focus, involvement of top management, process approach, and continual improvement.

ISO 27001:2013

Criteria for an information security management system (ISMS) to help organizations manage the security of assets that process or store critical and private information on finances, intellectual property, employee details, and clients / third parties.

ISO 14001:2015

Criteria for an environmental management system (EMS) mapping out a framework to follow in order to set up an effective EMS and ensuring environmental impact is measured and improved.

IT asset

Any company-owned system or hardware used in the course of business activities, including smartphones, tablets, laptops, or any other device with a serial number or unique asset tag.

IT asset disposition (ITAD)

Practice built around reusing, recycling, repurposing, repairing, or disposing of unwanted IT equipment in a safe and environmentally responsible way.

IT asset lifecycle

Series of stages an IT asset goes through during the span of its usable life, including planning, procurement, deployment, optimization, management, support, recovery, and disposition.

IT asset management (ITAM)

Set of business practices fulfilling the IT asset lifecycle for an organization; includes tracking IT asset location, deployment, maintenance, upgrades, and disposition as needed to optimize spending and support strategic decision-making within the IT environment.

IT asset recovery

Strategic process of reclaiming corporate-owned IT assets to maximize the value of those assets through repurposing, reselling, or responsible recycling.

IT asset recovery journey

Series of related steps an IT asset goes through during its recovery or reclamation process.

IT asset recovery program

Cohesive, company-wide policy outlining how company-owned IT assets are returned to the company when a device is lost or stolen, a device is upgraded, or in the event of an employee separation from the company, ensuring every device in the organization is recovered, processed, and disposed of through the same process.

IT asset recovery rate

Percentage of IT assets recovered out of IT assets eligible for recovery. Typically, the asset recovery rate is calculated for a specific project or over a specified period of time, such as one year.

IT service management (ITSM)

Collection of policies and processes used to plan, design, deliver, support, and improve the way a business uses information technology (IT) services.

Long-Term Evolution (LTE)

Standard for high-speed wireless communications, which increases the capacity and speed by using a different radio interference and an improved core network. Successor to 3G and predecessor to 4G connectivity.

managed mobility services (MMS)

IT and process management services required by a company to acquire, provision, and support mobile devices with integrated and/or wireless connectivity.

managed service provider (MSP)

Outsourced vendor or team providing regular support and services—such as network, application, infrastructure, and security—for customers via ongoing and regular support on the customer's premises, in the MSP's internal data center, or a third-party data center.

mobile application management (MAM)

Software and services that provision and control access to internally developed and commercially available mobile applications used in business settings on mobile IT assets.

mobile content management (MCM)

System responsible for storing and delivering content and services to mobile devices.

mobile device

Any electronic device small enough to be carried, enabled with wireless connectivity, and with the capacity for general computing; includes smartphones, tablets, and laptops.

mobile device policy

Set of rules companies establish that employees, contractors, and other personnel must adhere to, which communicates how devices are expected to be used within an organization.

mobile device management (MDM)

Software allowing the physical administration and securement of corporate-owned mobile devices. Predecessor to enterprise mobility management (EMM).

move, add, change, or delete (MACD)

Any move, hire, change, or removal of personnel affecting mobile services.

multifactor authentication (MFA)

IT security method requiring a user to provide two or more authentication factors to confirm their identity to gain access to corporate-owned IT assets, applications, networks, and servers.

National Institute of Standards and Technology (NIST) 800-88

Media sanitization guidelines—often referred to as NIST 800–88—providing robust guidance for erasing data from IT assets so any data found is irretrievable. NIST 800–88 is the most up-to-date and recommended level of data destruction.

original equipment manufacturer (OEM)

Company that assembles and manufactures physical IT assets.

physical security

Protection of personnel, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to an enterprise, agency, or institution, including protection from fire, flood, natural disasters, burglary, theft, vandalism, and terrorism.

Recovery Platform

Mobile reCell's proprietary software providing all the data, tools, and services necessary to give customers full access to and customization of their IT asset recovery programs.

resell revenue

Income received by a company from the resale of its recovered company-owned IT assets.

Responsible Recycling (R2) certification

Company-level certification based on the R2 Standard for the electronics recycling industry by Sustainable Electronics Recycling International (SERI), which strives to reuse and recycle devices to preserve resources, the environment, and the health and safety of workers and communities. R2 certification follows specific process requirements such as downstream recycling, data sanitization, testing and repair, materials recovery, specialty electronics, and brokering.

return on investment (ROI)

Financial analysis used to evaluate the efficiency of an investment or measure the probability of gaining a return from an investment.

return-ready kit

Individual or bulk IT asset recovery kit shipped to a specific end user or company location; includes everything required to return IT asset(s)—shipping materials and a prepaid shipping label. Return-ready kits are designed to fit one or more IT assets and ensure maximum safety during shipment.

Security Assertion Markup Language (SAML)

Open-standard data format used for exchanging authentication data between parties, typically an identity access management provider and a software or service provider.

security by design

Approach to software development seeking to make platforms as free of vulnerabilities and impervious to attack as possible through continuous testing, authentication safeguards, and adherence to programming best practices.

single sign-on (SSO)

User authentication service allowing a user to access multiple systems and/or applications with one set of login credentials.

software as a service (SaaS)

Model of software delivery and licensing in which software is accessed online and centrally hosted; often, pricing is tied to usage (consumption) or user count, per feature, tiered, or a flat rate.

software development kit (SDK)

Set of software development tools allowing for the creation of applications for a specific development platform.

software security

Protection of software applications and digital experiences from unauthorized access, use, or destruction.

subscriber identity module (SIM)

Circuit chip that securely stores an international mobile subscriber identity number and its related key, which identifies and authenticates IT asset users and stores their contacts and network access permissions; used in all Global System for Mobility (GSM) IT assets.

supply chain security

Part of supply chain management focusing on the risk management of external suppliers, vendors, logistics, and transportation. Its goal is to identify, analyze, and mitigate the risks inherent in working with other organizations as part of a supply chain, including both physical security relating to products and cybersecurity for software and services.

Sustainable Development Goals (SDG)

Adopted by the United Nations in 2015 as a universal call to action intended to end poverty, protect the environment and society, and ensure peace and prosperity by 2030.

sustainable solution

Solution developed to be long-lasting and environmentally responsible for the provider, the customer, and society as a whole.

System and Organization Controls (SOC) 2 Type 2

Report that examines a service organization's internal controls to secure and protect customer data over a duration of time.

technology expense management (TEM)

Management of technology costs such as software licenses, computer equipment, applications, and technology-related services, like software as a service (SaaS).

telecom expense management (TEM)

Management of an enterprise's total voice and data environment expenses and costs, including wireline and wireless technologies.

trade-in

Process in which a technology hardware or service provider offers discounts on new hardware and/or services in exchange for the customer returning their old hardware, which delivers more affordable devices to be resold in secondary markets or provides raw materials reused to make new IT assets more environmentally friendly. *See buyback.*

Trust Services Criteria (TSC)

Basic compliance checklist auditors reference during a SOC 2 audit around security, availability, processing integrity, confidentiality, and privacy; addresses logical and physical access controls, system operations, change management, and risk mitigations.

unified endpoint management (UEM)

Software allowing IT to manage, secure, and deploy corporate resources and applications on any IT asset from a single console; an evolution of, and replacement for, mobile device management (MDM) and enterprise mobility management (EMM).

user experience (UX)

Experience of a person using a service or product in terms of how easy it is to navigate or how pleasing it is to use.

value-added reseller (VAR)

Company that resells software, hardware, services, and/or third-party products in an effort to add value and resell them with additional offerings bundled in.

virtual private network (VPN)

Access method employing encryption to provide secure connectivity to remote IT assets over the internet.

wear your own device (WYOD)

Enterprise mobility program allowing end users to access business-related data and systems using individually owned wearable devices.

wireless carrier

Company selling wireless connectivity to customers for cellphone data and telephone calls. It may also be called a mobile network operator, mobile carrier, cellular company, or wireless service provider.

wireless carrier network

Collection of devices and underlying infrastructure used to transmit data from one location to another. The data transmission service is sold as a commodity, either directly to the end user or to a reseller.

wireless local area network (WLAN)

Wireless computer network linking two or more IT assets using a wireless distribution method within a limited area.

Zero Trust security infrastructure

Application where all programmatic requests and users must be authenticated, authorized, and continuously validated for security configuration before being granted access to applications or data.

mobile recell

Mobile reCell provides the leading software-driven solution for corporate-owned IT asset recovery, designed to help organizations ensure data security, automate manual processes, recover maximum value, and deliver a sustainable solution. The IT asset recovery platform provides complete visibility into asset shipment tracking, processing, and a secure chain of logistics as it automates the recovery, repurposing, reselling, and recycling of corporate-owned IT assets. Mobile reCell's success is driven by a commitment to deliver an unparalleled customer experience with unrivaled technology.

To learn more about Mobile reCell's solutions, visit mobilerecell.com.