

	POLICY	DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY	PO-IT-CORP-001	
		PAGE	REVISION DATE
		1 OF 12	01-JUN-2022

INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY

Approved by: André Grenier, Director, Information Technology 01-Jun-2022

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.

	POLICY	DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY	PO-IT-CORP-001	
		PAGE	REVISION DATE
		2 OF 12	01-JUN-2022

TABLE OF CONTENTS

1. Purpose	3
2. Scope	3
3. Accountabilities	3
3.1 Information Technology	3
3.2 Leaders	3
3.3 Accounts Payable	3
3.4 Human Resources	3
3.5 Employees	4
4. Definitions and Acronyms	4
5. Procedure	5
5.1 General Use	5
5.2 Hardware	5
5.3 Appropriate Use	5
5.4 Internet Use	5
5.5 Telephone Use	6
5.6 Electronic Mail (Email)	6
5.7 User Identification and Passwords	6
5.8 Mobility Devices	7
5.9 Social Media Guidelines	9
5.10 Audit	9
5.11 Audit Trails	9
5.12 Email	9
5.13 Security	9
5.14 Help and Support	10
5.15 Viruses and Spam	10
5.16 Privacy and Confidentiality	10
5.17 Licenses and Copyrights	10
5.18 Purchasing and Ownership	11
6. Supporting Documents	11
7. Interpretation and Updating	11

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.

	POLICY	DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY	PO-IT-CORP-001	
		PAGE	REVISION DATE
		3 OF 12	01-JUN-2022

8. Revision Record 12

1. Purpose

The objective of this policy is to protect CEDA's confidential information and processes from malicious computer viruses, spam and security breaches by establishing guidelines, standards and restrictions for all users of CEDA's information technologies, systems, software and networks.

2. Scope

CEDA is responsible for securing its systems and hardware against unauthorized access or abuse, while at the same time making them accessible to authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the consequences for not adhering to them. This policy applies to all employees and users of CEDA's systems and hardware.

CEDA maintains a cordial environment where personal growth and learning of the technology is encouraged. However, violations or any attempts to violate the provisions of this policy will result in disciplinary action, in accordance with CEDA's Discipline Policy, ranging from the temporary revocation of user access to termination of employment.

The users of CEDA's systems and hardware are responsible for respecting and adhering to all applicable laws related to the access and use of computer systems.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement and connectivity of mobile devices to any element of CEDA's systems.

3. Accountabilities

3.1 Information Technology

- Act as a resource for employees and leaders when there are any technology questions
- Technology recommendations are to be based on industry standards and best practices
- Defined approval steps must be followed for any access requests
- Established change control process to be followed for any system changes
- Data and system security applied to all solutions

3.2 Leaders

- Report any known policy violations of direct reports
- Ensure employees are not moving assigned assets without IT consent
- Involve IT when looking at third party technology solutions

3.3 Accounts Payable

- Flag any employee technology expense even if Leader has approved

3.4 Human Resources

- Approve investigation requests
- Approve access to personal information, by leaders, for active employees

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.

	POLICY	DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY	PO-IT-CORP-001	
		PAGE	REVISION DATE
		4 OF 12	01-JUN-2022

- Recommend and support action required for policy violations

3.5 Employees

- Understand, be familiar with, and comply with this policy

4. Definitions and Acronyms

APPLICABLE LAWS means any local, provincial, state, federal or international laws applicable to an activity in this policy.

CEDA means CEDA Parent Holdings Limited – all entities forming part of the CEDA Group of Companies.

CEDA BUSINESS means all work related activities engaged in by employees and subcontractors while working on CEDA or customer premises or CEDA worksites, participating in company-related social activities, in public while representing CEDA, or operating any vehicles leased or owned by CEDA (including heavy equipment) in conjunction with these activities.

EMPLOYEE includes any person employed by CEDA on a permanent full or part-time basis and independent contractors of CEDA (collectively “employees”) and employees of subcontractors providing services to CEDA or on behalf of CEDA.

HARDWARE means but is not limited to all electronic equipment owned, leased or rented by CEDA whether it is assigned to a particular employee or not, including but not limited to:

- Desktop/laptop/notebook/tablet computers
- Mobile phones including smartphones
- Printers, fax machines and photocopiers
- Landline telephones in all CEDA facilities and worksites
- Any electronic device capable of storing corporate data and connecting to an unmanaged network

IT means CEDA’s Information and Technology department.

oneCEDA INTRANET means the internal employee communication Intranet site.

SYSTEMS means but is not limited to any equipment, software, network, server or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that is owned/leased or rented by CEDA.

SOCIAL MEDIA refers to the means of interactions among people in which they create, share and/or exchange information and ideas in virtual communities and networking, including: Facebook, LinkedIn, Twitter, Instagram, blogging and all other social networking and connecting sites available on the Internet. Note: the absence or lack of explicit reference to a specific site does not limit the extent of this definition or application of this policy.

	POLICY		DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY		PO-IT-CORP-001	
			PAGE	REVISION DATE
			5 OF 12	01-JUN-2022

5. Procedure

5.1 General Use

All CEDA systems and hardware have been provided for CEDA business use. Employees may use CEDA systems and hardware for their personal use provided that it is done on the employee's personal time, such use is not interrupting computer service to others, and there is no potential damage to CEDA or our customers.

5.2 Hardware

- CEDA is the owner of all hardware provided. When departing the company, all assets including chargers must be returned.
- The cost of any missing assets may be allocated to the employee.
- Any hardware purchased by the employee that has been reimbursed (e.g. headsets) are the property of CEDA and expected to be returned in working order.
- No stickers of any kind, including CEDA branded stickers, are to be applied to any IT hardware without IT written approval. CEDA authorized stickers are the gold or blue asset tags and they are not to be tampered with.
- All possible care should be taken to keep the hardware in the condition it was received. Hardware has the potential to be reallocated at any time.

5.3 Appropriate Use

Employees at CEDA are encouraged to use the systems and hardware to further CEDA's goals and objectives. The types of activities that are encouraged include:

- Communicating with fellow employees, CEDA's business partners and customers within the context of an employee's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an employee's assigned responsibilities.
- Participating in educational or professional development activities.

5.4 Internet Use

Employees are to be aware that:

- Access to the Internet should include the use of good judgment, common sense and discretion. The Internet may not be used for illegal or unlawful purposes, including but not limited to: copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, competitive commercial activity unless pre-approved by CEDA, the dissemination of chain letters, computer tampering (e.g. spreading computer viruses) and the downloading of programs without approval by the IT department. Doing so can lead to disciplinary action up to and including termination of employment.
- The Internet, systems and hardware shall not be used in any way that violates CEDA's core values and policies. Employees should be aware that every Internet site you visit is capable of determining

	POLICY		DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY		PO-IT-CORP-001	
			PAGE	REVISION DATE
			6 OF 12	01-JUN-2022

who you are and who you represent. While non-CEDA business Internet browsing is not specifically prohibited, employees should limit their personal use of the Internet.

- Employees may not establish hardware as a participant in any peer-to-peer network, unless approved by CEDA's senior management.
- Use of CEDA's hardware in attempts to gain unauthorized access to remote systems is prohibited.
- Employees shall use all systems and hardware in compliance with their applicable proprietary rights and be aware that, in addition to disciplinary action, any violation of proprietary rights may result in the liability of the employee.

5.5 Telephone Use

Employees are to be aware that the telephone and mobility systems, including all analog and digital lines, are to be used for business purposes. Personal use is acceptable but should be limited.

5.6 Electronic Mail (Email)

- Use of work email is both a privilege and service provided to CEDA employees. Employees exercising this privilege are expected to act responsibly and respect the rights of others. Employees may use email for personal messages that do not amount to an unreasonable volume. Employees are encouraged to use the same personal and professional courtesies and considerations in email as they would in other forms of communication.
- CEDA often delivers official communications via email. As a result, employees with email work accounts are expected to check, manage, organize and clean their email accounts in a consistent and timely manner so that they are aware of important company announcements and updates as well as for fulfilling business and role-oriented tasks. Employees must manage their Inbox to remain within the mail box quota that is provided for their use.
- Employees are expected to remember that email sent from the company's email accounts reflects on the company. When using company email, employees are to comply with normal standards of professional and personal courtesy and conduct.

5.7 User Identification and Passwords

- User accounts are provided on an individual basis for individual use only. Sharing of user accounts and passwords is strictly prohibited.
- User identification and passwords are the primary form of user authentication used to grant access to CEDA's systems. To ensure passwords provide as much security as possible they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break thus allowing easier illicit access to CEDA's systems and thereby compromising the security of those systems.
- When creating a password, employees shall abide by the following guidelines in that all passwords:
 - Must be constructed according to set length and complexity requirements. As such passwords must be eight (8) characters in length and must include character type which includes upper or lower case, numbers and special character characters.
 - Will have a maximum lifespan of 180 days.

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.

	POLICY		DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY		PO-IT-CORP-001	
			PAGE	REVISION DATE
			7 OF 12	01-JUN-2022

- May not be reused any more frequently than every 12 password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
- Are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
- Are to be individually owned and kept confidential and are not to be shared under any circumstances.

5.8 Mobility Devices

CEDA may, with the approval the employee's Leader, issue a supported mobility device to enable and assist employees with performing their job functions. Mobility devices can include, but are not limited to: smartphones, tablets and cellular phones. CEDA recognizes the importance that mobile connectivity, media and applications play in many of its employees' lives and does not object to reasonable use of CEDA-issued mobility devices during an employee's non-working hours. All employees shall understand and abide by the following:

- Employees are personally liable and responsible for any application and media purchases that they make from their mobility device. CEDA will centrally license and distribute corporate supported applications. Corporate applications are company owned and distributed.
- Employees may not, under any circumstances, compromise the management or copyright controls on their device (ex. "jailbreaking" for Apple devices).
- Employees may not connect any non-CEDA issued mobility device to the CEDA network or systems under any circumstances.
- Texting and messaging should be used for business purposes. Reasonable personal use is acceptable but must not impede business productivity.
- A password must be maintained on the mobility device at all times. After 10 failed password attempts to log into the device, the device will be automatically wiped of all user information. Passwords must be kept private. Do not share passwords with anyone, write them down or use them in public or common areas without adequate precautions.
- Employees will immediately report lost or stolen devices (police report must be submitted).
- Employees will immediately report any suspected or actual incidents of unauthorized data access or data loss.
- As part of the management controls within the mobile device portion of this policy:
 - Location data from the device may be tracked by CEDA.
 - CEDA may track and inspect the contents of any CEDA issued mobility device.
 - CEDA may monitor and audit access to corporate resources.
 - CEDA reserves the right to wipe all data from the mobile device in the event of a device being lost or stolen, or for policy non-compliance. Where possible, reasonable attempts will be made to preserve personal data on the device. However, if CEDA deems it necessary, a full device wipe will be issued.
- Employees are permitted to purchase and install personal applications and media on their mobility device with the following considerations:
 - Peer-to-peer file sharing applications are not allowed.

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.

	POLICY		DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY		PO-IT-CORP-001	
			PAGE	REVISION DATE
			8 OF 12	01-JUN-2022

- Unsanctioned cloud-based applications may not be used with corporate data.
- Unsanctioned instant messaging applications may not be used to discuss company business.
- Third party email applications may not be used to conduct company business.
- Employees may backup data and media from their device to their CEDA computer. If software is required to support the device (i.e. iTunes), the employee can contact the CEDA IT Service Desk to assist with the installation. Backup to CEDA network drives and the cloud is prohibited.
- Under this policy, CEDA employees are eligible for a new or replacement device every 36 months. It is the employee's responsibility to provide the appropriate care and responsibility to ensure the device is in proper working order for this time period. CEDA will provide protective cases for employees that work in hazardous areas.

Meraki Systems Manager is software used by CEDA to manage and secure mobility devices. The software tracks device information, such as the version of the operating system (OS) for CEDA to maintain compliance. Also, the software provides a way for CEDA to wipe the device clean of all company information when an employee leaves the company for any reason, or if the device is lost or stolen. It also monitors required security measures such as password length and complexity to maintain compliance. It is the expectation that employees follow all procedures outlined in this policy, regardless of whether technology controls are available and enforced for their devices.

Cameras

- Mobility devices are now equipped with cameras and the software to record pictures and videos. It is the employee's responsibility to understand if the customer site they are working has a policy that does not allow cameras. If that is the case, the employee must inform CEDA IT to disable the camera on their mobility device, or not take that device onsite if it cannot be disabled.
- Employees shall refrain from taking and/or publishing pictures or videos of CEDA employees, sites, processes and tools unless directly for business purposes and with the written approval of their Leader and the respective employees.

Mobile Phone Numbers

- Employees can, at their request, transfer a personal number to their CEDA mobility device. However, employees should understand that, following the transfer, that phone number is now property of CEDA. Reasonable efforts will be made to return that number to the employee at their request, but return is not guaranteed.

Non-Compliance

- Employees shall use all Systems and Hardware in compliance with their applicable proprietary rights and be aware that, in addition to disciplinary action, any violation of proprietary rights may result in the liability of the Employee.
- Failure to comply with any part of the IT policy, whether enforced by technology controls or not, can result in loss of access to corporate resources and a partial or full wipe of the mobility device.

	POLICY	DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY	PO-IT-CORP-001	
		PAGE	REVISION DATE
		9 OF 12	01-JUN-2022

5.9 Social Media Guidelines

CEDA recognizes the role social media plays in many of its employees' lives and does not object to reasonable use during the employee's non-working hours. When used inappropriately, social media can cause harm to the company and create liability on behalf of the employee to CEDA or a third party. We encourage all employees to review and understand CEDA's Social Media Guidelines.

5.10 Audit

- Employees should have no expectation of privacy while using any CEDA systems or hardware. CEDA monitors all internet activity occurring on CEDA systems and hardware.
- CEDA reserves the right to audit employee activity on CEDA systems and hardware including the use of email, messaging, texting and Internet at any time without the consent of the employee.
- In addition to any audit that may occur, CEDA employs filtering software to limit access to sites on the Internet. If CEDA discovers activities that do not comply with applicable laws or departmental policies, records retrieved may be used to document the wrongful content.

5.11 Audit Trails

IT can and will establish audit trails and these will be accessed, published and used without notice. Such audit trails will be able to track the attachment of an external device to a computer and the resulting reports may be used for investigation of possible breaches and or misuse. The employee agrees to and accepts that his or her access and or connection to CEDA systems may be monitored to record dates, times, duration of access, etc., to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains CEDA's highest priority.

5.12 Email

- Please be aware that CEDA owns any communication sent via company email, messaging, texting or Internet that is stored on equipment owned or leased by CEDA.
- CEDA maintains the right to at any time access any material in your company email or on your hardware that is supplied by CEDA.

5.13 Security

- All employees shall immediately report to IT any potential virus or security breach of a CEDA system or hardware or any possible infringement of this policy.
- All employees are required to use CEDA approved two-factor authentication (2FA) to access CEDA's systems externally. To further enhance security, CEDA recommends that any system accessed from CEDA hardware uses 2FA (i.e. if you access your online banking from CEDA's hardware, you should enable the 2FA feature from your banking provider).
- CEDA also recommends that employees use 2FA in their personal lives wherever possible to better protect themselves in the ever-growing cybercrime environment.

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.

	POLICY		DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY		PO-IT-CORP-001	
			PAGE	REVISION DATE
			10 OF 12	01-JUN-2022

5.14 Help and Support

- IT will support CEDA sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT department.
- Employees will make no modifications of any kind to CEDA's systems and hardware without written approval from IT. This includes, but is not limited to any reconfiguration of CEDA hardware.
- IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

5.15 Viruses and Spam

- To prevent viruses from unconfirmed programs, email attachments and other sources, employees must have the most current version of virus protection software enabled on their CEDA issued hardware.
- Employees are not to adjust or tamper with any components of the virus protection product installed on their hardware.
- An employee shall call the CEDA IT Service Desk if he or she is uncomfortable with the contents of any software that may have been obtained from an external source.
- Employees are to avoid opening any attachments, emails, documents, or product installs that they are not certain about and refer to the CEDA IT Service Desk for assistance.

5.16 Privacy and Confidentiality

- Information is a company asset and must be appropriately managed to ensure its confidentiality, integrity, and availability. Employees and other authorized users are empowered to use CEDA's hardware and systems in a manner appropriate to their security classification to effectively perform their jobs. It is the responsibility of all employees and other authorized users to ensure information is protected from unauthorized modification, destruction, or disclosure, whether accidental or intentional.
- All information used in the operation of CEDA is CEDA's property. All software developed by CEDA employees or contract personnel on behalf of CEDA, or purchased by CEDA, is also CEDA's property.

5.17 Licenses and Copyrights

- Everyone must adhere to software license agreements and respect copyrights on all material including product obtained through the Internet. All product, both software and hardware (including any electronic devices being hooked up or otherwise connected to company hardware) must be approved by IT.
- All software installed on CEDA hardware including any smartphones, tablets and other electronic devices must be approved by IT.
- All software requests must be forwarded to IT for their review prior to any installation.
- If software is found on any CEDA hardware without approval from IT, this software is subject to removal without consent from any party or individual.

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.

	POLICY	DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY	PO-IT-CORP-001	
		PAGE	REVISION DATE
		11 OF 12	01-JUN-2022

5.18 Purchasing and Ownership

- All hardware, software and systems provided or obtained through CEDA is the property of CEDA. No personal hardware, software or systems are permissible.
- The IT department will coordinate all software and hardware purchases, licensing control and related activities to ensure CEDA is in compliance with all legal regulations.
- If there is a requirement for software that is not currently available, that request should be made to the CEDA IT Service Desk. Requests will be evaluated based on the following criteria:
 - Business need
 - Software is free of cost, or required approvals are in place
 - Lack of an internally supplied alternative
 - Security impact to CEDA systems
 - Software is free of Viruses and other malware
- Unauthorized downloading or uploading of any type of software, including software available from the Internet is prohibited.
- Personal or non-compliant hardware purchases or use is also prohibited.
- Periodic software and hardware audits will be conducted by the IT department to determine compliance with licensing agreements and any unauthorized or illegal software discovered will be removed from the computer system.
- All phone numbers provided by CEDA for use by land phones, mobile phone or/and smartphones are the property of CEDA.
- Transfer of files or data onto USB's, CD's or other electronic media, or transfer to personal or non-related business computers is prohibited unless it is intended for CEDA business use only. Upon departure of a CEDA employee, all email and phone line will be forwarded to the person's immediate Leader.

6. Supporting Documents

Document Name	Document Identification	Revision
Social Media Guidelines	GD-IT-CORP-001	Latest Revision
Discipline Policy	n/a	Latest Revision
Hybrid Work Arrangement Policy	PO-HR-CORP-014	Latest Revision

7. Interpretation and Updating

The Director, Information Technology is accountable for responding to any requests for clarification and for regular review and updating of this policy.

	POLICY	DOCUMENT ID	
	INFORMATION SYSTEMS AND TECHNOLOGY ACCEPTABLE USE POLICY	PO-IT-CORP-001	
		PAGE	REVISION DATE
		12 OF 12	01-JUN-2022

8. Revision Record

Revision Date	Section Affected	Changes Made
DEC-17-2011	All	Issued for Implementation
DEC-15-2014	n/a	Revisions
JUN-01-2022	All	Revisions

PRINTED COPIES OF THIS DOCUMENT ARE CONSIDERED UNCONTROLLED/INFORMATION ONLY COPIES. THE CONTROLLED VERSION IS LOCATED ON CEDA'S INTRANET. THIS DOCUMENT MAY NOT BE COPIED OR REPRODUCED IN ANY FORM WITHOUT THE EXPRESS WRITTEN CONSENT OF CEDA.