#BeeraSharp

Digital Rights and Security Toolkit for Ugandan Businesses

Funded by the European Union

Enabel

Table of Contents

Introduction

Welcome to Your #BeeraSharp Digital Rights Toolkit

In Uganda's rapidly evolving digital landscape, businesses face significant challenges in safeguarding their digital operations against surveillance, internet restrictions, and cyber threats. These vulnerabilities become particularly pronounced during politically sensitive periods, such as elections.

About The #BeeraSharp Toolkit

The #BeeraSharp Digital Rights Toolkit for businesses is a comprehensive resource designed to equip business owners, innovators, and entrepreneurs in Uganda with practical knowledge and skills to navigate the digital ecosystem safely and responsibly. Aligned with the UN Guiding Principles on Business and Human Rights, this toolkit addresses the growing challenges related to digital rights, data protection, cybersecurity, and digital surveillance that businesses face in Uganda's evolving digital landscape.

Available in both online and offline formats, the toolkit provides step-by-step guidance, practical tools, and contextually relevant examples to help businesses protect their digital operations while respecting the rights of their customers and employees. It features checklists, templates, case studies, and actionable guidance across eight core competencies related to digital rights and business operations.

This resource is designed to bridge the existing knowledge gap and support businesses in fostering responsible, rights-respecting practices while contributing to broader national and regional efforts to create a sustainable, equitable, and rights-based business environment.

Why Digital Rights Matter for Your Business

As a business owner in Uganda, digital rights impact:

- Your ability to conduct secure financial transactions
- Protection of your customer data
- Security of your business communications
- Access to critical online services
- Business continuity during internet restrictions
- Protection from fraud and cyber threats

Recent incidents in Uganda, including social media shutdowns during the 2016 elections and a nationwide internet blackout in the 2021 elections, demonstrate the importance of digital preparedness. These events, alongside increasing evidence of sophisticated surveillance tools being deployed, create significant risks for businesses that rely on digital technologies.

Key Beneficiaries

This toolkit specifically targets a diverse range of stakeholders in Uganda's digital landscape. Its primary focus is on Micro, Small, and Medium Enterprises (MSMEs) that make up 90% of Uganda's private sector and often face significant digital skills gaps.[1] Uganda's expansive informal economy contributes approximately 50 percent to the national GDP. The rise of technology and digital platforms highlights the evolving and dynamic nature of this sector.

The toolkit is designed to serve the expansive informal economy, including mobile money operators who handle sensitive financial data, tech entrepreneurs driving innovation, and traditional businesses adopting digital tools to stay competitive in this ever changing digital landscape.

Beneficiaries
Micro, Small, and Medium Enterprises (MSMEs) - Representing 90% of Uganda's private sector, these businesses often lack digital skills and resources to protect themselves online.
Mobile Money Agents and Operators - Businesses handling financial transactions through mobile platforms who need to understand security protocols and customer data protection.
Tech Entrepreneurs and Startups - Innovators developing digital products who need to understand how to build rights-respecting technologies.
Traditional Businesses Adopting Digital Tools - Established businesses transitioning to digital operations, who need guidance on new digital risks.
Business Owners with Limited Digital Literacy - Entrepreneurs using basic digital tools (like feature phones) who need simple, accessible security guidance.

[1] https://[illegible]

Why This Toolkit is Needed

Uganda's digital rights landscape presents significant challenges for businesses operating in the digital space. Despite progress in responsible business conduct, human rights violations persist due to weak regulatory frameworks. As digital adoption accelerates, new risks have emerged—from data privacy breaches to surveillance concerns and computer systems making biased decisions.

Business and Human Rights Context Businesses play a critical role in promoting and protecting human rights, yet many enterprises, particularly in developing contexts like Uganda, struggle with limited awareness, capacity, and tools to uphold these responsibilities effectively. While notable progress has been made in advancing responsible business conduct, human rights violations and abuses persist within business operations.

Growing Digital Vulnerability As businesses increasingly adopt digital tools, platforms, and data-driven technologies, new risks to human rights have emerged, ranging from surveillance and data privacy breaches to online exploitation, digital discrimination, algorithmic bias, and silencing dissenting voices through platform manipulation or content moderation policies.

Skills Gap and Capacity Challenges Approximately 72% of MSMEs in Uganda suffer from a digital skills gap, making them vulnerable to online threats.[4] Many businesses lack awareness of digital rights principles and security practices, leaving them ill-equipped to recognize, prevent, or respond to digital rights violations tied to business operations.

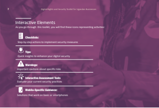
Regulatory and Political Environment Uganda has experienced internet shutdowns during elections (2016 and 2021) and the implementation of social media taxes, creating unpredictable operating conditions for businesses reliant on digital communications. Mobile money transactions have also been affected during shutdowns. These recent incidents, alongside increasing evidence of sophisticated surveillance tools being deployed, create significant risks for businesses that rely on digital technologies.

Weak Institutional Frameworks Weak institutional capacity, fragmented coordination among state and non-state actors, and the absence of robust regulatory frameworks make it difficult to enforce human rights compliance in the digital sphere. Many businesses lack internal accountability mechanisms for digital rights protection.

Gender-Specific and Marginalised Group Challenges The toolkit addresses identified gaps in digital equality, with special attention given to gender-specific challenges and inclusion of vulnerable and marginalised groups, as well as Persons with Disabilities who face unique circumstances in the digital space.

Need for Practical, Accessible Guidance Without clear frameworks or tools adapted to the Ugandan context, many stakeholders are ill-equipped to navigate the complex intersection of digital rights and business operations. This toolkit aims to bridge this knowledge gap by providing accessible, action-oriented guidance tailored to the unique realities of Uganda's business environment.

[4] [illegible]



Interactive Elements

As you go through this toolkit, you will find these icons representing activities:

Checklists:
Step-by-step actions to implement security measures

Tips:
Quick insights to enhance your digital security

Warnings:
Important cautions about specific risks

Interactive Assessment Tools
Evaluate your current security practices

Mobile-Specific Guidance:
Solutions that work on basic or smartphones

How to Apply This Toolkit

This toolkit is designed for all Ugandan businesses, regardless of their digital maturity. To get started, first **ASSESS** your vulnerabilities using the toolkit assessment on page 24. Then **PRIORITISE** protecting your most sensitive data and critical systems. Finally, **ACT** by implementing quick security wins that require minimal resources. Simply find your business type (agent, *MSMEs*, Larger *Enterprise*, or startup) in the Table of *Contents* below to locate the sections most relevant to your needs.

Business Agents	SME's	Larger Enterprises	Startups
Focus on:	**Focus on:**	**Focus on:**	**Focus on:**
Mobile Device Security	Customer Data	Website Protection	Compliance
Transaction Protection	Social Media Accounts	Data Storage	Advanced Threats
Fraud Prevention	Payment Systems	Online Communications	System Security
Start Here:	**Start Here:**	**Start Here:**	**Start Here:**
Mobile Security (p.19)	Consent Forms (p.12)	Website Security (p.27)	Rights Fundamentals (p.8)
Feature Phones (p.21)	Password Security (p.14)	Data Protection (p.11)	AI Security (p.20)
Common Scams (p.20)	Social Media (p.29)	Cloud Security (p.18)	Rights Checklist (p.30)

Digital Rights Fundamentals

Human Rights in the Digital Age

Digital rights are an extension of fundamental human rights into the online world. Just as people are entitled to rights in the physical world, these rights must also be upheld in digital spaces. Digital rights empower individuals to access, use, create, and share digital content, and to use technologies like computers, mobile devices, and the internet freely and securely. They safeguard essential freedoms such as expression, privacy, and access to information. For businesses that collect data, monitor communications, or deliver digital services, respecting these rights is a vital responsibility, protecting users, employees, and communities while building trust and accountability.

According to the United Nations Guiding Principles on Business and Human Rights,[a] companies are responsible for upholding human rights in all environments, including the digital realm. This includes safeguarding:

- Privacy: Protection from unauthorised surveillance and misuse of personal data
- Freedom of Expression: Ability to communicate and access information freely
- Equality and Non-discrimination: Fair treatment free from algorithmic bias
- Access to Information: Right to receive and share information digitally
- Freedom of Assembly: Participation in online communities and movements
- Due Process: Fairness in digital decisions, including contesting automated outcomes

For businesses in Uganda's digital economy, respecting digital rights is crucial to meet legal obligations and to earn customer trust, protect reputation, and support a fair digital future.

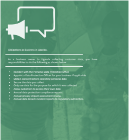
Key Digital Rights in Business Contexts:

- Data Privacy: The right of individuals to control how their personal information is collected, used, and shared.
- Digital Security: The right to secure digital communications and protection from cyber threats.
- Access to Information: The right to seek, receive, and impart information and ideas through digital channels.
- Freedom from Surveillance: Protection from unnecessary monitoring of online activities and communications.
- Consent and Control: The right to make informed choices about digital engagement and data sharing.
- Digital Equality: Non-discrimination in access to digital technologies and services.
- Transparency: The right to understand how digital systems operate and make decisions.
- Right to Be Forgotten: The ability to have certain personal information removed from internet searches and directories.

Key Laws and Regulations

1. Data Protection and Privacy Act (2019):[4] Governs how personal data should be collected, processed, and stored
2. Computer Misuse Act:[5] Regulates the improper use of computer systems
3. Uganda Communications Act:[6] Governs telecommunications and internet service providers
4. Electronic Transactions Act:[7] Provides for the use, security, and regulation of electronic communications

Your Obligations as a Business in Uganda



Obligations as Business in Uganda.

As a business owner in Uganda collecting customer data, you have responsibilities to do the following as shown below:

- Register with the Personal Data Protection Office
- Appoint a Data Protection Officer for your business if applicable
- Obtain consent before collecting personal data
- Secure the data you collect
- Only use data for the purpose for which it was collected
- Allow customers to access their own data
- Annual data protection compliance reports.
- Annual privacy impact assessment review.
- Annual data breach incident reports to regulatory authorities.

Digital Tools and Their Rights Implications

Different digital tools present unique rights considerations that businesses should be able to address, as shown below:

Digital Tool	Common Business Use	Rights Implications
Mobile Money	Payment Processing	Financial privacy, security of transactions.
Social Media	Marketing, customer engagement	Data collection, content moderation, surveillance
Customer Databases	Customer relationship engagement	Data protection, security, consent management
Cloud Services	Data storage, business operations	Data sovereignty, third-party access
Surveillance Cameras	Security monitoring	Privacy, data autonomy, excessive monitoring
Biometric Systems	Access control, identification	Privacy, consent, security of sensitive data
Websites & Apps	Service delivery, e-commerce	Cookie tracking, surveillance, data collection and protection, accessibility
Digital Communication	Internal and external communication	Confidentiality, encryption, surveillance
AI & Algorithms	Automation, decision-making, geo-AI, sorting	Transparency, discrimination, fairness

Digital Rights in Practice

Case Study: Mobile Money Business in Kampala

Nassali runs a mobile money business in Kampala. After learning about data protection requirements, she implemented simple changes:

- Created a privacy policy and displayed it at her shop
- Started using a password-protected spreadsheet to record transactions instead of a notebook
- Began deleting customer transaction details after completing the necessary reporting
- Installed an app lock on her phone to protect customer information
- These simple changes helped protect her customers and her business from potential data breaches.

Data Protection and Privacy

Understanding Data Protection

For businesses, data protection involves safeguarding the personal information of your customers, employees, and partners. This includes names, contact information, financial details, and any other identifying information.

What is Personally Identifiable Information (PII)

Personally Identifiable Information (PII)

As a business owner in Uganda, you need to know that PII includes any data that can be used to identify an individual, such as:

- Names
- Phone numbers
- Email addresses
- National ID numbers (NIN)
- Location data
- Biometric data (fingerprints, facial recognition)
- Financial information

Digital/Human Rights Risk Checklist

This checklist assists MSMEs in identifying and mitigating digital and human rights risks associated with their products and services. Its purpose is to enhance user protection, foster trust, and ensure compliance with ethical business standards in Uganda.

- *Have you identified potential risks to stored user data (e.g., unauthorised access, breaches) and applied encryption or other safeguards to mitigate them?*
- *Have you considered the risk of excluding users with disabilities when designing or delivering your product or service and taken steps to make it accessible to them?*
- *Have you assessed the risks of collecting more personal data than is necessary and taken steps to limit data collection to only what is essential for your service?*

To evaluate your product/services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

Data Protection Checklist for Your Business

Essential Steps for Data Protection: To evaluate the data protections that your product/services offer, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here: *https://assessment.threats.org/*

Biometric Data Considerations

Suppose your business collects biometric data (fingerprints, facial recognition, etc.), like Nassali, for example, who runs a mobile money kiosk in Kampala, now captures photos of customers making large transactions. She will need to clearly explain this security measure, obtain explicit consent, and store the biometric data securely with access controls.

Special Requirements Apply

Below are a few ideas on what to consider when dealing with special requirements for collecting biometric data from users and customers.

- You must obtain explicit consent
- You need stronger security measures
- You should have a clear purpose for the collection
- You must provide alternatives for those who don't want to provide biometric data

Obtaining Informed Consent

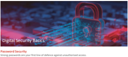
Before collecting customer data, you need informed consent:

Sample Consent Statement:

> *"At [Your Business Name], we collect your [specific data types] to [purpose of collection]. We protect your information and will not share it without your permission except as required by law. You can view, correct, or delete your data by contacting us at [contact information]."*

Tip: *Make your consent forms simple and clear. Avoid complex legal language that customers won't understand.*

To evaluate the biometric data considerations that your business offers, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.thrcets.org/*



Digital Security Basics

Password Security

Strong passwords are your first line of defence against unauthorised access.

Creating Strong Passwords

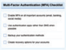
- Use at least 12 characters
- Include uppercase and lowercase letters, numbers, and symbols
- Avoid personal information (birthdates, names)
- Use different passwords for different accounts
- Consider using a password manager

For Feature Phones: Even with basic phones, use PIN codes and avoid obvious combinations like "1234" or your birthdate.

Authentication Best Practices

Strong authentication practices are a good defence against digital threats: use unique, complex passwords for each account, enable multi-factor authentication wherever available, and consider password managers to securely store credentials.

Multi-Factor Authentication (MFA) Checklist:



Multi-Factor Authentication (MFA) Checklist

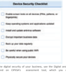
- ☐ Enable MFA on all important accounts (email, banking, social media)
- ☐ Use authentication apps rather than SMS when possible
- ☐ Backup your authentication methods
- ☐ Create recovery options for your accounts

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.thrarts.org/*

Device Security

Keep your business devices secure with these essential steps:

Device Security Checklist:



Device Security Checklist

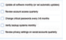
- □ Enable screen locks on all devices (PINs, patterns, or fingerprints)
- □ Keep operating systems and applications updated
- □ Install and update antivirus software
- □ Encrypt important business data
- □ Back up your data regularly
- □ Be careful when using public WiFi
- □ Physically secure your devices

To evaluate the digital security of your business, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.thraets.org/*

Security Maintenance

Regular maintenance is essential for ongoing security:

Regular Security Practices:



Regular Security Practices

- □ Update all software monthly (or set automatic updates)
- □ Review account access quarterly
- □ Change critical passwords every 3-6 months
- □ Verify backup systems monthly
- □ Review privacy settings on social accounts quarterly

To evaluate and see how the digital security of your business can be made better, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.thraets.org/*

Secure Communications

Communication Security Basics

As a business, your communications may contain sensitive information about your operations, finances, and customers. Securing these communications is essential.

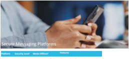
Understanding Encryption

Encryption is like a secret code that makes your messages unreadable to anyone except the intended recipient.

Types of Encryption:

- End-to-End Encryption: Only you and your recipient can read messages
- Transport Layer Encryption: Protects data as it travels across the internet

To evaluate the digital communications of your business, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*



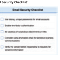
Secure Messaging Platforms

Platform	Security Level	Works Offline?	Features
Signal	Very High	No	End-to-end encryption, disappearing messages
WhatsApp	High	No	End-to-end encryption, disappearing messages, business features which additionally offer two-step verification (2SV), device login alerts, and auto log-out on linked devices for enhanced account protection, etc
Telegram	Moderate	No	Secret chats are encrypted

Tip: *For maximum security in WhatsApp, verify security codes with important business contacts and enable two-step verification.*

Email and Cloud Security

Email and Cloud Security Checklist:



Email Security Checklist

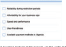
- □ Use strong, unique passwords for email accounts
- □ Enable two-factor authentication
- □ Be cautious of suspicious attachments or links
- □ Consider using encrypted email for sensitive business communications
- □ Verify the sender before responding to requests for sensitive information

To evaluate the digital communications of your business, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.throets.org/*

Using VPNs for Business

A Virtual Private Network (VPN) creates a secure connection to the internet, which is especially important when using public WiFi or during internet restrictions.

VPN Selection Criteria for Ugandan Businesses:

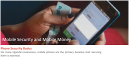


VPN Selection Criteria for Ugandan Businesses

- □ Reliability during restriction periods
- □ Affordability for your business size
- □ Speed and performance
- □ User-friendliness
- □ Available payment methods in Uganda

Warning: *Free VPNs often collect and sell your data. It's worth investing in a reputable paid service for your business.*

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.throets.org/*

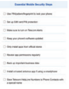


Mobile Security and Mobile Money

Phone Security Basics

For many Ugandan businesses, mobile phones are the primary business tool. Securing them is essential.

Essential Mobile Security Steps:



Essential Mobile Security Steps

□ Use PIN/pattern/fingerprint to lock your phone

□ Set up SIM card PIN protection

□ Make sure to turn on Telecom alerts

□ Keep your phone's software updated

□ Only install apps from official stores

□ Review app permissions regularly

□ Back up important business data

□ Install a trusted antivirus app if using a smartphone

□ Save Telecom HelpLine Numbers to Phone Contacts with a special name

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

Beware of These Common Scams:

Common Scams

Below are a few examples of common scams that you should be aware of as a business in Uganda. These might not be exhaustive but are common ones.

- Calls claiming you sent money to the wrong person
- Messages saying you've won a prize
- Requests to share your PIN "for verification"
- Impersonation of mobile money call center employees
- Fake mobile money agent numbers
- Smishing - SMS messages with phishing links.

Feature Phone Security

Many businesses in Uganda use feature phones rather than smartphones. Security is still possible:

Security for Basic Phones

Below are a few examples of common security basics for dealing with basic or feature phones that could help your business.

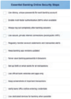
- Enable PIN protection
- Use call privacy settings
- Save USSD prompts e.g *160# etc to avoid mistakes.
- Delete sensitive SMS messages
- Don't store critical information on the phone
- Be cautious of sharing your phone with others

Banking Online Security and Digital Banking

Digital Banking Security Basics

For Ugandan businesses using online banking services, securing your digital financial transactions is essential for protecting business funds, customer payments, and sensitive financial data.

Essential Banking Online Security Steps:



Essential Banking Online Security Steps
□ Use strong, unique passwords for each banking account
□ Enable multi-factor authentication (MFA) when available
□ Always log out completely after banking sessions
□ Use secure, private internet connections (avoid public WiFi)
□ Regularly monitor account statements and transaction alerts
□ Keep banking app versions updated
□ Never save banking passwords in browsers
□ Set up SMS or email alerts for all transactions
□ Use official bank websites and apps only
□ Keep screenshots of important transactions
□ Verify bank URLs before entering credentials
□ Use dedicated devices for banking when possible

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

Beware of These Common Banking Scams:

Common Banking Online Scams

Below are a few examples of common banking scams that you should be aware of as a business in Uganda. These might not be exhaustive but are common ones.

- Fake bank websites requesting login credentials.
- Phishing emails claiming account suspension or verification needed
- SMS messages asking you to "update" banking information via links.
- Calls impersonating bank staff requesting PINS or passwords.
- Social engineering attacks claiming urgent account issues.
- Fraudulent loan approval messages requiring upfront payments.
- Man-in-the-middle attacks on unsecured WiFi networks.

Banks will never ask for your full PIN, password, or security codes via phone, email, or SMS. Always contact your bank using official numbers: Stanbic Bank (0800 250 250), Centenary Bank (0800 200 555), DFCU Bank (0800 300 255) to verify suspicious communications.

Digital Surveillance and Protection

Understanding Digital Surveillance

Digital surveillance involves monitoring your online activities, communications, and data. In Uganda, surveillance can come from various sources and may affect your business operations.

Types of Surveillance to Be Aware Of

- Network monitoring: Tracking internet traffic
- Mobile surveillance: Monitoring phone calls, messages, and location
- Social media monitoring: Tracking business and personal accounts
- Location tracking: Following physical movements through digital means

Signs Your Business May Be Under Surveillance

Watch for These Warning Signs:

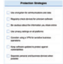
Warning Signs

Below are a few examples of signs that could give a hint when your business could be under surveillance.

- Unusual battery drain on devices
- Unexpected phone behaviour (heating up, strange noises during calls)
- Unknown applications or processes running
- Suspicious network activity
- Unrecognized account logins
- Unusual customer inquiries or information requests

Basic Anti-Surveillance Measures

Protection Strategies



Protection Strategies

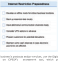
- □ Use encryption for communications and data
- □ Regularly check devices for unknown software
- □ Be cautious about the information you share online
- □ Use privacy settings on all platforms
- □ Consider using a VPN for sensitive business operations
- □ Keep software updated to protect against vulnerabilities
- □ Separate personal and business devices when possible

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.thraets.org/*

Operating During Internet Restrictions

Internet shutdowns and social media blocks have occurred in Uganda, particularly during elections. Businesses should prepare for these disruptions.

Internet Restriction Preparedness



Internet Restriction Preparedness

□ Develop an offline mode for critical business functions

□ Back up essential data locally

□ Have alternative communication channels ready

□ Consider VPN options in advance

□ Prepare customers for potential disruptions

□ Maintain some cash reserves in case electronic payments are affected

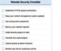
To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

Managing Online Presence

Website Security

If your business has a website, securing it is crucial for protecting your online presence and customer data.

Website Security Checklist



Website Security Checklist

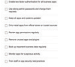
- ☐ Implement HTTPS (secure connection)
- ☐ Keep your content management system updated
- ☐ Use strong admin passwords
- ☐ Backup your website regularly
- ☐ Install security plugins or tools
- ☐ Uninstall non-useful plugins
- ☐ Control access to admin functions
- ☐ Monitor your site for suspicious activity

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

App Security

If your business uses mobile applications, securing them is crucial for protecting your business operations, customer data and maintaining user trust.

App Security Checklist



Essential App Security Steps

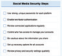
- □ Enable two factor authentication for all business apps
- □ Use strong admin passwords and change them regularly
- □ Keep all apps and systems updated
- □ Only install apps from official stores or trusted sources
- □ Review app permissions regularly
- □ Remove unused apps and plugins
- □ Back up important business data regularly
- □ Monitor apps for suspicious activity
- □ Train staff on app security best practices

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

Social Media Account Security

Social media accounts represent your business online and need protection.

Social Media Security Steps



Social Media Security Steps

- □ Use strong, unique passwords for each platform
- □ Enable two-factor authentication
- □ Review connected applications regularly
- □ Control who has access to manage your accounts
- □ Be cautious about the information you share
- □ Set up recovery options for all accounts
- □ Review privacy and security settings quarterly

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

Content Protection

Protect your business's digital content with these measures:

- Consider watermarking important images
- Understand copyright protection for your content
- Be careful about what customer information you share
- Have a plan for responding to negative or false information
- Monitor mentions of your business online

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESA's assessment tool, which you can find here *https://assessment.threats.org/*

Emerging Technologies and AI

AI Tools for Business

Artificial intelligence (AI) tools offer opportunities for Ugandan businesses but come with security and privacy considerations.

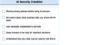
Potential Business Uses

- Consider watermarking important images
- Understand copyright protection for your content
- Be careful about what customer information you share
- Have a plan for responding to negative or false information
- Monitor mentions of your business online

AI Risk Checklist

When using AI tools, keep these risk factors in mind:

AI Security Checklist



AI Security Checklist

□ Review privacy policies before using AI services

□ Be careful about what business data you share with AI tools

□ Use reputable, established AI services

□ Keep humans in the loop for important decisions

□ Understand how your data may be used to train the AI

To evaluate your business's products and/or services, use the Digital and Human Rights Checklist found on CIPESK's assessment tool, which you can find here *https://assessment.throats.org/*

Detecting AI-Generated Threats

AI can be used to create sophisticated scams targeting businesses:

Watch for These AI-Enhanced Threats:

AI-Enhanced Threats.

Below are a few examples of artificial intelligence-enhanced threats and trends currently ongoing.

- Deepfake videos or audio impersonating business partners
- Highly convincing phishing messages
- AI-generated fraud attempts
- Fake reviews or social media posts

Emergency Response Plan

Preparing for Digital Security Incidents

Every business should have a plan for responding to digital security incidents.

Digital Security Response Plan Template:

Action	Activities
1. Identify the Problem:	What Systems are affected? What data might be compromised? Who needs to be informed?
2. Contain the Issue	Disconnect affected systems Change compromised passwords Secure physical devices
3. Resolve and Recover	Remove malicious software Restore from backups if needed Report to authorities if necessary
4. Learn and Improve	Document what happened Identify security gaps Implement new protections

Key Emergency Contacts

Keep these contacts accessible in case of digital security emergencies:

Uganda Police Cybercrime Unit: 112 or 999
Your Internet Service Provider: *MTN*, *Airtel*, Zuku, Canalbox, and more
Mobile Money Provider Fraud Line: MTN - 0771 001 000 Airtel - +256200202003
Uganda Computer Emergency Response Team: *roles and contacts*
Uganda Banks Contacts: Stanbic Bank (+256 312 224 600, 0800 250 250), Centenary Bank (0800 200 555, +256 317 202 315, WhatsApp +256 744 200 555), DFCU Bank (0800 100 255), Standard Chartered Bank ((+256)313294100 (If calling from abroad)/ (+256)200524100(, and Absa Bank (+256 312 218 348, WhatsApp +256 707 433 433). *More Banks*

Resources and Tools

Recommended Tools

Tool Type
Password Managers
VPN Services
Encryption Tools
Secure Messaging
Antivirus
Backup Solutions

Further Learning

For more information about digital rights and security, consult these resources:

https://secresearch.tacticaltech.org/
https://ssd.eff.org/
https://tco.nita.go.ug/
https://foundation.mozilla.org/en/privacynotincluded/articles/how-to-protect-your-privacy-from-chatgpt-and-other-ai-chatbots/
https://www.accessnow.org/guide/internet-shutdowns-and-elections-handbook/
https://www.frontlinedefenders.org/en/digital-security-resources

Important Organizations

Connect with these organisations working on digital rights in Uganda:

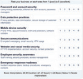
- **Collaboration on International ICT Policy for East and Southern Africa (CIPESA)** - *http://cipesa.org*
- **The Unwanted Witness** - *https://www.unwantedwitness.org*
- **Defend Defenders** - *https://defenddefenders.org*
- **Defenders Protection Initiative** - *https://www.defendersprotection.org*

Connect with these regulatory organisations

- **Uganda Communication Commission (UCC) - https://www.ucc.co.ug**
- **Personal Data Protection Office - https://www.pdpo.go.ug**
- **National Information Technology Authority - https://www.nita.go.ug**

Digital Rights Toolkit Assessment

Use this quick assessment to evaluate your business's digital security readiness. This Digital Rights Toolkit Assessment helps Ugandan business owners quickly evaluate their digital security across seven key areas. By rating each area from 1-5, businesses receive a total score that identifies their security level and highlights vulnerabilities requiring immediate attention.



Digital Rights Toolkit Assessment

Rate your business's digital security readiness

Rate your business on each area from 1 (poor) to 5 (excellent)					
Password and account security Using strong passwords, different for each account, password managers	1	2	3	4	5
Data protection practices Privacy policies, data minimization, secure storage of customer information	1	2	3	4	5
Mobile device security Phone PINs, app permissions, SIM card protection, software updates	1	2	3	4	5
Secure communications Encrypted messaging, email security, VPN usage	1	2	3	4	5
Website and social media security HTTPS implementation, account security, content protection	1	2	3	4	5
Employee security awareness Staff training, security protocols, access management	1	2	3	4	5
Emergency response readiness Incident response plans, backup procedures, emergency contacts	1	2	3	4	5

Score Interpretation: 28-35 Excellent | 21-27 Good | 14-20 Basic | Below 14 Needs Improvement

Use your score to prioritise which sections of this toolkit to implement first. Focus on areas where you scored lowest, as these represent your greatest vulnerabilities. Begin with quick security wins that can immediately strengthen your business's digital protection while developing a long-term plan for comprehensive improvement.

Key Terms and Concepts

Essential digital rights terminology in simplified language	
Key Term	**Definition**
Digital Rights	Human rights that protect people in the online world, including privacy, freedom of expression, and access to information.
Biometric Data	Physical characteristics used to identify individuals, such as fingerprints, facial features, or voice patterns.
Personally Identifiable Information (PII)	Any data that can identify a specific person, like names, phone numbers, ID numbers, or locations.
Data Protection	Steps taken to keep personal information safe from unauthorised access, theft, or misuse.
Encryption	Technology that scrambles information so only authorised people can read it, like a secret code for your data.
Multi-Factor Authentication (MFA)	Security process requiring two or more proofs of identity (like a password plus a code sent to your phone).
VPN (Virtual Private Network)	Tool that creates a secure, private connection to the internet, hiding your activities from others.
End-to-End Encryption	Security method where only the sender and recipient can read messages, not even the service provider.
Digital Surveillance	Monitoring of people's online activities, communications, and data, often without their knowledge.
Informed Consent	Permission given by a person after fully understanding what data is being collected and how it will be used.
Data Minimization	Practice of collecting only the minimum amount of personal information needed for a specific purpose.
Phishing	Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.
Malware	Harmful software designed to damage or gain unauthorised access to computers or phones.
Internet Shutdowns	Deliberate disruption of internet access by authorities, often during elections or protests.
Deepfake	Artificially created videos or audio recordings that make it appear someone did or said something they didn't.
Data Breach	Incident where confidential information is accessed without authorisation.
Smishing	SMS phishing - scam text messages that trick you into sharing personal information or clicking dangerous links.
Data Protection Officer	Person responsible for overseeing data protection strategy and implementation in an organization.

Digital Equality	Equal access to digital technologies and services for all people, without discrimination.
Right to Be Forgotten	Right to have certain personal information removed from internet searches and directories.

The #BeeraSharp ("be smart" in Luganda) campaign is dedicated towards addressing the gaps that Ugandan businesses face when navigating digital rights, online spaces and digital data. The campaign aims to fill key knowledge gaps on the understanding of business legal obligations through adopting secure and ethical digital practices to build a smarter, safer, and more resilient business ecosystem in Uganda. Join the #BeeraSharp campaign and share your thoughts on how to navigate safely as businesses in Uganda! For more details visit: *https://cipesa.org/beera-sharp/*

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 108 Katalima Crescent, Naguru.| P.O.Box 122311,Kampala (U)
☎+256 414 289 502| programmes@cipesa.org| @cipesaug
www.cipesa.org