# ICT Security Bulletin

Sept 2020
Vol.1

For more information contact your IT Support

You can also contact IT Security department on: itsecu@delta.co.zw Or Ext 33211 33233

## EMPLOYEE ACCEPTABLE USE

Over the course of an average working day, a Delta employee handles a great deal of information. While that information can come in different formats, it has one thing in common: it is an asset for the Company – and potentially a very valuable one. At Delta, we take our commitment to protecting the Company's non-public information seriously.

**Acceptable Use Details and Requirements**

- Employee Acceptable Use (EAU) instructs Users of their responsibilities and obligations for appropriately using non-public Company information, systems, and using good cybersecurity behaviours. This document should be followed in combination with the Information Protection Policy. A violation of Employee Acceptable Use may result in disciplinary action up to and including termination of employment or service contract. Violation of Employee Acceptable Use may also be a violation of other Company policies or procedures, including, but not limited to the Company Code of Business Conduct.

- All Systems and any Company information or messages stored, created, sent, or received using them are the property of the Company.

### USE OF COMPANY SYSTEMS

- DO use only authorized devices and appropriately licensed software to access non-public Company information, systems and technology infrastructure.

- DO NOT attempt to circumvent or alter security on any Company system. Possessing, developing or attempting to use malicious software and hacker tools for these purposes is prohibited.

DO keep current with system updates and security patches for Company systems and as directed by Information Technology.

- DO NOT automatically forward or archive Company business email on non-Company systems.

- DO return all Company assets issued to you prior to leaving the Company. Assets include mobile devices, removable storage media, badges, keys, ID cards, software, digital data, operations manuals, and other Company related documentation.

**Personal Use & Monitoring**

- Company systems are to be used for business. Occasional personal use is permitted as long as it does not impact your job responsibilities, violate the EAU, other Company policies or any applicable laws.
- The Company may monitor any system and your use of any system according with applicable Company procedures and applicable legal requirements.
- Except as protected by applicable law, your communications on Company Systems are not private. Any data gathered because of monitoring activities may be disclosed outside the Company in support or as part of investigations or legal proceedings.

### SECURE COMPANY INFORMATION

**Classifying**

Protect non-public Company information like any other valuable Company asset. Mark sensitive Company information with the correct classification label so that it can be handled and protected appropriately.
The Company classifies its sensitive information as follows:

### CONFIDENTIAL

Annual Business Plans
Consumer Intelligence
Department Budgets
Bottler Price Lists
Contract Proposals
Sales Forecasts

### PERSONAL INFORMATION

Email Address
Employee ID Number
Name

### SENSITIVE PERSONAL INFORMATION (SPI)

Biometric Information
Credit Card Number
Bank Account Number
Government ID Number
Health/ Medical Information
Passport Information

### HIGHLY RESTRICTED

Pre-release Financials
Acquisition Plans
Strategic Business Plans
Planned Global Media Spends
Product Formulas
Ingredient Information

# ICT Security Bulletin

Sept 2020
Vol.1

For more information contact your IT Support

You can also contact IT Security department on:

itsecu@delta.co.zw

Or Ext 33211

33233

## EMPLOYEE ACCEPTABLE USE

### Sharing

- Obtain approval from the Business Owner before authorizing access to, sharing, disclosing, or transmitting Company classified information.
- A non-disclosure agreement (NDA) must be signed by third parties that will be exposed to classified Company information.
- Store non-public Company information only on authorized Company systems.
- Do not share or store classified information on third party or non-Company systems unless a contractual agreement to protect the information exists.
- If you are not sure information can be shared or how to share it, ask your manager or legal counsel.

### Safeguarding

- Keep work and public areas clear of classified Company information when not present or not in use.
- Always activate the screen lock on computers and other mobile devices when away from your desk or not in use.
- Secure or take with you the keys or access codes to filing cabinets, desk drawers, offices and other storage

## PRACTICE CYBER HYGIENE

### Protect Your Identity

- You are responsible for the activity that occurs under your Company-issued user ID.
- Do not disclose or allow others to use your access credentials.
- Create strong passwords and passphrases: keep them private: do not reuse them; and change them when required.
- Do not share passwords between your work and private user accounts.
- Do not use your Company email address for private, non-business related use.

### Protect Non-Public Company Information

- Label information with the correct classification.
- Use the right protections. Store Highly Restricted and Sensitive Personal Information on encrypted removable storage media approved by Strategic Security.
- Non-public Company information stays with the Company. You cannot take Company information with you when you leave the Company.

### Use Approved Applications and Services

- Use Company provided software to connect to the Company business network, where possible.
- Never use unsecured, public wireless networks and risk sensitive info being accessed inappropriately.

### Share and Control Information Appropriately

- Share info only with those with access and need-to-know.

### Ask for outside parties to sign a non-disclosure agreement (NDA) before giving access.

- Be conscious of your surroundings when discussing information and activities in public spaces.
- Watch what you share in your personal use of social media. Our Company's Information Protection Policy, Insider Trading Policy, and other policies still apply.

### Protect Your Devices

- Keep applications and software up-to-date. Do not delay restarting your devices after updates.
- Make regular backups. Store backup data in a secure location so if your devices are lost or stolen, Company information is not lost.
- Never leave devices unattended in public locations.
- Secure laptops, removable storage media and mobile devices when not in use.
- Immediately report lost or stolen devices to your local IT Support and Loss Control.

### Terms You Should Know

User: an employee, contingent worker, vendor, contractor, or other authorized person who uses a Company system for their daily work.

Non-public Company Information: Company information not disclosed or made generally available to the public. Non-public information examples include presentations, spreadsheets,
project documentation, emails or videos.

System: refers to all computers, laptops, tablets, mobile devices, servers, network and communication systems.

Technology Infrastructure: system supporting the delivery of business systems and IT-enabled processes, which are owned, leased, operated, or contracted by the Company.

A non-Company system: home or private computers,
public Internet terminals or kiosks, third party applications, etc.

Removable Storage Media: back-up tapes, removable
hard drives; cartridges, DAT, VHS, CD, DVD, flash memory cards, USB flash drives, and thumb key drive

**Remember:**

Encrypt Data: Always encrypt information classified
as Highly Restricted or SPI. Failure to properly encrypt documents may result in a data loss prevention inquiry and/ or automatic encryption of document contents.

Data Disposal: Follow secure disposal practices for non-public Company information that is no longer needed. Use cross-shredder or authorized secure disposal services. For electronic media,
permanently delete information before disposing of or reusing media.

Business Owner: executive officer accountable for a defined category of classified Company information.

Encryption: process to make information hidden or secret and prevents any inadvertent access or unauthorized disclosure.