Exchange for Change

Information Management & Security Procedure

1. Scope **1**
2. Aims **1**
3. Responsibilities **2**
4. What is Information? **2**
5. Receiving Information **3**
6. Managing Documented Information **3**
7. Passwords and data security **4**
Remote Access 4
BYOD 4
Potential/Actual System security breach notification 4
8. Other relevant Exchange for Change information **5**
Software Updates 5
Disaster Recovery 5
9. CDS Portal Access and Password Reset Procedure **5**
Password Reset 7
10. Office Access & Swipe Card controls **7**
11. Change History and Approval **8**
Appendix 1 – Portal Users **1**

1. Scope

This policy applies to all information whether hardcopy or electronic that is created, managed and maintained by EFC, including WHS related information. Information management & security is a complex series of controls that include:

- the provision of suitable hardware to ensure ongoing reliability and access to data as required to perform daily activities.
- the provision of software that enables information to be captured and securely stored but prevents unauthorised access.
- the management of the information or data from when it is received or created, until the information is destroyed, deleted or permanently archived.

All EFC employees must comply with this procedure to the degree everyone is responsible for information.

2. Aims

The aim of this procedure is to ensure all business-related information is managed so that it can be relied upon as evidence that EFC responsibilities are being managed and delivered in accordance with planned arrangements. Effective management of information should therefore take into consideration appropriate identification, storage, access, retention and disposal. Business related records may include financial, customer, employee, WHS and systems records, in any format including hardcopy and electronic.

3. Responsibilities

All staff of EFC are responsible for:

- maintaining policies, procedures, instructions and guidelines sufficient to ensure work is carried out in controlled conditions.
- managing work related information in accordance with procedures, policies and statutory requirements.
- generating records as evidence of their activities and outputs
- capturing data, records, reports and other evidence into a records management system
- protecting information, data and records from unauthorised access or destruction.

The Office Administrator is responsible for maintaining hardcopy records in a safe and accessible location and provide a SharePoint folder structure as a repository for electronic records.

SeekTech is EFC's outsourced Network Administrator, with expertise in managing networks, access, data backup and user support. SeekTech is responsible to:

- ensure all servers, mainframes and other network equipment is secured with adequate ventilation and secured access.
- ensure that data back-ups are conducted every night and a copy of the backed-up data is kept in an offsite location. Their details are:

  help@seektech.com.au
  Phone 08 7123 6000
  Level 1, 336 South Rd
  Richmond SA 5033
  www.seektech.com.au

Staff, especially managers, are encouraged to read this policy in conjunction with other relevant Exchange for Change policies, located on the EFC SharePoint document repository.

4. What is Information?

In the context of this procedure, information is knowledge that is generated, documented, received, and maintained as evidence or for knowledge preservation purposes by EFC, to meet legal obligations or required in the conduct of business.

Information may commence life as system generated data, regulatory requirements, emails or verbal instruction. If this information needs to be retained due to being work-related, it may be converted into a documented policy or procedure, or entered into a blank form, or saved as an electronic report.

Information therefore has a life-cycle as follows:

KNOWLEDGE → DATA/DOCUMENT → RECORD → ARCHIVE/BACKUP

At each stage of the life-cycle, the information must remain secured. For example, confidentiality requirements must be considered during conversations with other people regarding EFC operations; printed information regarding EFC or the CDS must not be left on desks or printers where the information might be accessed by visitors, cleaners etc.

5. Receiving Information

Any employee receiving work related information has a responsibility to ensure it is captured in the most appropriate format. Information will typically be captured by:

- sending an email (if received verbally)
- generating a report (if held in system software)
- creating a documented policy or procedure (if used to provide guidance to others)

Examples of business related information that follow the information life cycle through to becoming a record may include:

- Completed Forms
- Meeting Minutes
- Reports
- Plans
- Inspection Records
- Project Documents
- Submissions
- Approved Procedures (originals only)
- Safe Work Method Statements
- Risk Assessments
- Emails, etc.

The purpose of a record is for knowledge preservation. Therefore, Exchange for Change will determine if draft documents and other work in progress material is to be kept as a record.

6. Managing Documented Information

Exchange for Change is a small business and as such will determine what processes need to be reflected within documented procedures. All documented procedures are prepared using an EFC template and are reviewed and approved by the appropriate authority within the management team. Company-wide policies and procedures will be approved by the CEO whereas some department-based procedures can be approved by the department Manager, ensuring a management team member always approves an EFC procedure as a minimum.

As part of the consultative arrangements within EFC, feedback from any employee or contractor will be considered and incorporated where applicable, to ensure these documents remain relevant, practical and appropriate. This is particularly critical to WHS related documents to ensure workers' needs are always considered.

Approved documents will be stored within the relevant SharePoint folder for access by employees. A record of approval of an EFC document may include physical signature or an email notification, a copy of which will be retained.

All staff are encouraged to access and use the SharePoint version of procedures rather than save them locally or print them, to avoid using a superseded version.

7. Passwords and data security

As an additional layer of security to business-related data, passwords are utilised to access all critical or confidential information. All employees must log in using an alpha-numeric password which must be updated at least every 3 months (this is forced by the system).

Where an employee forgets the password or is ‘locked out’ after five attempts, SeekTech is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

Passwords are not to be shared or displayed anywhere that can be seen by anyone else.

The EFC office can only be accessed using a security pass and therefore PC’s/laptops may be left unattended during the day for meetings/lunch etc. although must be locked and secured at the end of the working day. If laptops cannot be locked to the desk at night, they must be locked in a drawer or cabinet.

Computers must not be left on overnight or during absence of the owner unless the system forces the user to log-in after a reasonable time (e.g. 30 minutes).

Access to the CDS data portal is only achieved through password, including employees, suppliers and MRF’s.

Due to the scope of the business, confidential Supplier and other stakeholder information is held within reports and spreadsheets etc. Where this data needs to be transmitted electronically, passwords or encryption of data will be performed to prevent access by other unintended parties.

All information used within EFC is to adhere to the privacy laws and confidentiality requirements. Any employee breaching this may have their employment terminated.

Remote Access

Most EFC employees have remote access to the EFC network including SharePoint, email and cloud-based applications. The same security controls apply when working remotely or from home, so that information on a mobile phone or laptop cannot be accessed without the appropriate authority.

BYOD

Employees are not required to bring their own device for work purposes. All hardware and software will be provided to address the needs of each role. Therefore, employees are not to transfer and store data to their own device as this can create a security risk as well as a risk of transferring a virus.

Potential/Actual System security breach notification

IT Service providers are contractually required to monitor IT systems for any unauthorised access and report to EFC of any security breach/attempted breach.

The EFC must as soon as practicable report to the State any breach (or attempted breach) of, or unauthorised access to, the EFC's security and back-up systems. Where there has been a breach or unauthorised access to the EFC's security and back-up systems, the EFC must prepare and implement a corrective action plan approved by the State Representative.

8. Other relevant Exchange for Change information

SharePoint folders will hold copies of other documents received from external sources, where access to the external sources is limited via password and/or registration (e.g. publications, standards etc). Where 3rd party websites maintain controlled documents (e.g. NSW EPA protocols and procedures), these will be accessed directly from their website to prevent using obsolete versions, wherever possible.

Copies of contractor agreements and related operational records are held within a SharePoint folder, other than information and data managed via the EFC portal.

Software Updates

All Exchange for Change employees utilise a desktop or laptop computer for daily work activities. These computers receive systems and security updates on a regular basis via the contracted IT support business Seek Tech (www.seektech.com.au).

In order to ensure updates are deployed all employees must “restart” their computers weekly (i.e. shutting down does not deploy updates), typically Friday evening or Monday morning.

Disaster Recovery

EFC has documented Business Continuity and Disaster Recovery Plans within the SharePoint library which covers disaster recovery.

9. CDS Portal Access and Password Reset Procedure

EfC CDS portal is an Oracle based database used by various Scheme Participants.

As described in the Portal Architecture Design under heading Portal User Access Management & Data Security there are various roles for various scheme participants. The scheme participants can be broadly defined into 6 key stakeholders as shown below:

Stakeholder	Portal Access Role Code
Scheme Coordinator	Can be view, edit and admin
Network Operator	Currently has no access to the portal
Material Recovery Facilities [MRF]	Can be view and edit
Beverage Suppliers	Can be view and edit
Exporters	Can be view and edit
NSW EPA & ACT No Waste	Can be view only

For each of these stakeholders to receive access, the following procedure is followed:

Scheme Coordinator:

The functional responsibility of the portal lies with the Scheme Coordinator and thus the following 4 roles can be granted based on the roles and responsibilities of each individual as defined in their job description.

- Supplier Operation – This access is only granted to the Commercial Manager
- SC Administrator – This access is granted to individuals responsible to generate monthly invoices and view and edit supplier and MRF data if required.
- SC Operation – This access is granted to anyone who can access and edit supplier and MRF data in the portal when needed
- SC Viewer – This is a view only access and is granted to anyone who liaises with suppliers and MRF and require to only view the existing data in the portal.

Procedure to request & grant access:

- Based on the role and responsibilities of an individual, the team leader will initiate an approval request to the CEO along with the reason for the required access.
- Once approval has been received the user access will be set up by the Commercial team and details of the same will be sent to the user in 2 separate emails, one containing the username and the other the password to maintain security.

Appendix 1 of this procedure has a list of EFC staff that have Portal access and the level of access.

Network Operator – Currently the Network Operator does not have any access to the CDS portal since they do not submit their data in the portal but through an agreed SIE platform or via e-mail.

Material Recovery Facilities [MRFs], Beverage Suppliers & Exporters – They are end users of the portal and are required to enter data on a monthly basis and edit the same if required. Thus, they may need access to edit or view data as necessary.

Procedure to request & grant access:

- The MRFs, Suppliers and exporters are initially contacted by the Beverage Supplier Support team to nominate one or more portal users by providing the following details:
  First Name:
  Last Name:
  E-mail Address:
  Full Company Name:
  Scheme:
- Once details have been received, the same is entered in a shared document listing all existing portal users.
- The user is then created and tagged to only one organisation and one scheme as mentioned in the above details.
- The user logins are tested and once successful the password is reset prior to emailing details to the user.
- Login details are sent in 3 emails, one introducing the scheme with the user manual, second contains the username and third containing the password.
- If an existing supplier requires an additional user at a later time, then either the existing user must request access for the additional user or anyone of a higher authority from the supplier's company must request access for the additional user. The higher authority can be the manager or anyone in a similar capacity of the additional user.

NSW EPA & ACT No Waste – They are end users of the portal and will be granted view only access to the data of the requested MRF. They are restricted from accessing supplier data in the capacity of the Scheme Coordinator and thus must request the data from the Scheme Coordinator as and when required.

Procedure to request and grant portal access:

- The requestor will send an email to the Scheme Coordinator Commercial Manager who will review the access and further obtain approval for the CEO of the Scheme Coordinator.
- Once approval has been received the Commercial Manager or anyone in the similar capacity will create the user in the portal.
- The user details in 2 separate emails, one containing the username and the other the password to maintain security

Password Reset

Any stakeholders mentioned in this document can request portal password reset by following the below procedure:

- When a portal user logs in to the CDS portal using their credentials and receive an authentication failure error message, they may require a password reset.
- All users are requested to email portalsupport@exchnageforchange.com.au with their user details and request for a password reset.
- The Scheme Coordinator's Beverage Supplier Contact team will reset the requestor's password, test the same and send a separate e-mail containing the new password to the user's e-mail address as recorded in the portal.
- In case the password reset functionality is not working then the Scheme Coordinator contacts the IT Service Provider to investigate the same and meanwhile reset any user's password in case it is urgent.

10. Office Access & Swipe Card controls

Access to EFC Rhodes office is controlled by a proximity card. Proximity cards have a unique identifier which allows cards to only provide access to specified areas of the office. The Office Manager controls the issuing of cards and recording who has been allocated each individual card.

All EFC staff are issued a proximity card by the Office Administrator when they commence employment with EFC. When an employee ceases employment with EFC the office administrator will retrieve the card from the individual.

Contractors that will be based in EFC office for an extended period of time maybe issued a proximity card that has same access rights as a EFC staff member. The decision to issue a contractor with a staff card will be for any of EFC Executive Management team.

Guest maybe issued a Guest Card while they are based in EFC office. This card will only have access to the front door of the office. The decision on issuing a Guest Card will be for any of EFC Executive Management team.

If a card is lost or not retrieved from an ex-employee, the Office Administrator will de-activate the associated card.

11. Change History and Approval

Revision	Date	Change Summary	Next Review date
0.0	24th August 2018	1st issue	
1.0	2nd Oct 2018	Added requirement to restart computers weekly and additional guidance on passwords.	30th June 2019
2.0	Dec 2018	Update to incorporate data security to the scope of the procedure.	30th June 2019
2.1	19th June 2019	Clarification to system security breach notification procedure.	30th June 2019

Prepared by:

Mark Grovenor
EFC Audit Manager

Approved by:

Peter Bruce
EFC Chief Executive Officer

Appendix 1 – Portal Users

User Login	First Name	Last Name	Email	Organisation Nam	Login Role
heath.warman@exchangeforchange.com.au	Heath	Warman	heath.warman@exchangeforchange.com.au	EFC	Supplier_Operation
senthil.sundararajan@exchangeforchange.com.au	Senthil	Sundararajan	senthil.sundararajan@exchangeforchange.com.au	EFC	SC_Viewer
nikita.nagpal@exchangeforchange.com.au	Nikita	Nagpal	nikita.nagpal@exchangeforchange.com.au	EFC	SC_Operation
argie.calibo@exchangeforchange.com.au	Argie	Calibo	argie.calibo@exchangeforchange.com.au	EFC	SC_Administrator
cassandra.bruce@exchangeforchange.com.au	Cassandra	Bruce	cassandra.bruce@exchangeforchange.com.au	EFC	SC_Administrator
Katphyn.Vong@exchangeforchange.com.au	Katphyn	Vong	Katphyn.Vong@exchangeforchange.com.au	EFC	SC_Administrator
Zohal.Sultanzada@exchangeforchange.com.au	Zohal	Sultanzada	Zohal.Sultanzada@exchangeforchange.com.au	EFC	SC_Administrator
Richard.parramon@exchangeforchange.com.au	Richard	Parramon	Richard.parramon@exchangeforchange.com.au	EFC	SC_Administrator

Current Scheme Coordinator portal users as on 05.06.19