AGEL adviseurs
ruimte
infra
bouw
milieu

Memo

Datum	:	30 mei 2018
Bestemd voor	:	Evelien Philipse – Eversdijk
Van	:	Ton-Ewout van Dalen Paraaf :
Projectnummer	:	20170765
Betreft	:	**LTG Technology Services Europe B.V., Grenssteen 33 Breda, zaaknummer 18032305 (aanvullende gegevens)**

- De bij de aanvraag behorende tekeningen zijn toegevoegd aan het OLO-dossier;
- De soorten te verwerken elektronica zijn beschreven in de herziene toelichting op de aanvraag D02, paragraaf 2.2;
- Voor wat betreft de capaciteit van de opgeslagen gevaarlijke stoffen wordt verwezen naar de herziene toelichting D02 op de aanvraag, paragraaf 8.2;
- Voor wat betreft de procedures van acceptatie, controle en verwerking van de ontvangen afvalstoffen wordt verwezen naar de bijgaande Engelstalige procedurebeschrijvingen afkomstig van de aanvrager. Voor een beter begrip is hierna een korte samenvatting en verduidelijking opgenomen met een verwijzing/opsomming naar/van de procedurebeschrijvingen.
- Een afschrift van het besluit op de vormvrije mer-beoordeling is toegevoegd aan het OLO-dossier
- Technische informatie m.b.t. de shredderinstallatie is aan het OLO-dossier toegevoegd. Voor wat betreft de capaciteit van de shredder wordt verwezen naar de herziene toelichting D02 op de aanvraag, paragraaf 2.2;
- De AEIRUS-berekening is aan het OLO-dossier toegevoegd;
- De procesbeschrijving zoals opgenomen in de vormvrije mer-beoordeling is het OLO-dossier toegevoegd;
- De worst-case berekening luchtkwaliteit is aan het OLO-dossier toegevoegd.

Normec CO₂-PRESTATIELADDER Normec VCA* Normec ISO 9001 ISO 9001

Postbus 4156
4900 CD Oosterhout
Hoevestein 20b
4903 SC Oosterhout

t. 0162 - 456481
f. 0162 - 435588
e. info@ageladviseurs.nl
i. www.ageladviseurs.nl

Op alle door ons aanvaarde opdrachten en verrichte werkzaamheden zijn de 'De rechtsverhouding opdrachtgever-architect, ingenieur en adviseur DNR 2011 herzien (juli 2013)' van toepassing. De DNR 2011 herzien (juli 2013) wordt op verzoek toegezonden.
BTW nr. NL800203823B01 - IBAN NL72ABNA0594482291 - BIC ABNANL2A - KvK Breda 20051141

Samenvatting:

Administratieve organisatie en interne controle (AO/IC) en acceptatie- en verwerkingsbeleid (A&V)

Het systeem voor AO/IC en A&V-beleid binnen de inrichting is samenhangend beschreven in de volgende documenten:

bijlage 1.	LTG Technology Services Europe BV (RE-TECK) - Waste acceptance policy
bijlage 2.	Waste Overview and processing route
bijlage 3.	Receiving of goods in control
bijlage 4.	Internal Audit
bijlage 5.	Corrective actions
bijlage 6.	IT-security concept
bijlage 7.	Resource usage instructions
bijlage 8.	Battery Handling
bijlage 9.	Receiving, Sorting, separating - visual process

Met bijlagen wordt door de inrichting een samenhangend geheel gegeven tussen het systeem van de administratieve organisatie en interne controle enerzijds en het acceptatie- en verwerkingsbeleid anderzijds.
Het geheel heeft betrekking op de acceptatie en verwerking (niet limitatief) van Smartphones, mobiele telefoons, tablets, laptops , IPod, e-reader enzovoorts. Het gehele acceptatie- en verwerkingsbeleid is uitgewerkt in bijlage 1, waarbij in hoofdstuk 3.0 van de betreffende bijlage is beschreven dat niet juist verpakte afvalstoffen niet worden geaccepteerd. Het bedrijf zal gevaarlijke afvalstoffen (zijnde batterijen, laptops, telefoons etc.) accepteren zoals opgenomen in de bijlage. Mochten niet juist verpakte afvalstoffen binnen de inrichting aanwezig zijn, wordt de vervoerder direct geïnformeerd over de vervolgstappen en worden deze afvalstoffen door hiervoor erkende inzamelaars uit de inrichting afgevoerd om de tijd dat deze afvalstoffen binnen de inrichting aanwezig zijn te minimaliseren.
Klanten van de inrichting zijn op de hoogte van het acceptatie- en verwerkingsbeleid van de inrichting en zijn hiermee ook bekend welke afvalstoffen niet ingenomen worden. Dit beleid maakt onderdeel uit van de contracten van de inrichting met haar klanten, waarmee de vooracceptatie feitelijk geborgd is.

Om het voor medewerkers begrijpelijk te maken zijn kritieke momenten, werkwijzen en procedures ook visueel gemaakt. Zie hiervoor bijvoorbeeld bijlage 3 waarin naast de beschrijving de kritieke momenten ook met foto's zijn gevisualiseerd. Aanvullende voorbeelden hiervoor zijn ook bijlage 8 voor de behandeling van lithium en niet lithium batterijen en bijlage 9 waarin een voorbeeld is opgenomen vanaf de ontvangst, verwerking, sortering en shredderen en het proces van batterij pack.

De interne audit binnen de inrichting is vastgelegd in bijlage 4 en de corrigerende acties zijn beschreven in bijlage 5. Hiermee kan het AO/IC systeem binnen de inrichting worden beheerst en waar nodig worden bijgestuurd.
De beveiliging van computersystemen tegen ongeautoriseerd gebruik en tegen verlies van gegevens is in bijlage 6 opgenomen.

In bijlage 2 wordt naar Eural code gescheiden inzicht gegeven in verschillende te accepteren afvalstoffen en de daarbij behorende proces(verwerkings)routes.
In bijlage 7 is daarnaast nog een procedure beschreven om zo zorgvuldig mogelijk om te gaan met de grondstoffen in de te verwerken afvalstoffen om hergebruik van grondstoffen te maximaliseren en het ontstaan van afvalstoffen te minimaliseren.

Het gehele systeem van de administratieve organisatie en interne controle (AO/IC) en het acceptatie- en verwerkingsbeleid (A&V) zal onderdeel uit gaan maken van de managementsystemen ISO 9001:2015, ISO 14001:2015, OHSAS 18001:2007, R2:2013 en RIOS:2006 en tevens het WEELABEX certificaat. Hiervoor moet de inrichting echter in werking zijn om deze systemen gecertificeerd te krijgen en het WEELABEX certificaat te behalen. Met deze systemen en certificaat wordt het geheel daarmee onafhankelijk geborgd.

Bijlage 1

LTG Technology Services Europe BV(RE-TECK) WASTE ACCEPTANCE POLICY

Electronic discard is one of the fastest growing segments of today's world. Recycling raw materials from end-of-life electronics is the most effective solution to the growing e-waste problem. Most electronic devices contain a variety of materials, including metals that can be recovered for future uses. Re-teck does dismantling of electronics products and provide best reuse possibilities, intact natural resources are conserved and air and water pollution caused by hazardous disposal is avoided. Additionally, recycling reduces the amount of greenhouse gas emissions caused by the manufacturing of new products.

1.0 WASTE ACCEPTED BY RE-TECK

1.1 E-Waste

1.1.1 **Re-teck. accepts electronic wastes from OEM's generated in the production faults, customer return products and not repairable, and failed in factory testing and damaged in the handling**. Re-Teck's waste acceptance practices and policies are based upon global policy, and local laws followed for e-*waste.*

1.1.2 **Electronics wastes including, but not limited to:**

1.1.2.1 Smart phones, Mobile phones, Tablets, Laptops , Ipod, e-reader etc.

2.0 WASTE ACCEPTED BY RE-TECK ONLY WITH PRIOR CHARACTERIZATION AND APPROVAL

2.1 Electronic waste which has been characterized by Original equipment manufacturer and criteria to accepted the electronic waste following approval by Re-Teck according to the Re-Teck Waste Acceptance Protocol. A list of all equipment and devices with part number, manufacturer name, and trade or brand name for each product is necessary for waste characterization and approval by Re-Teck. *Re-Teck, does not accepts any other hazardous waste.*

3.0 NON-CONFORMING WASTES NOT ACCEPTED BY RE-TECK

3.1 Improper Packaging: The supplier shall not tender and Re-Teck, shall not knowingly accept or collect for transportation any container which:

a. is not sealed and properly labelled;
b. is punctured or materially damaged;
c. is overfilled or overweight (see below);
d. contains anything other than electronics waste;
e. contains radioactive materials
f. requires special handling specified by the supplier.

3.2 Re-teck does not accept any Hazardous Waste including, but not limited to:

3.2.1 Materials contaminated with chemical and biological agents
3.2.2 Cathode Ray Tubes in any condition
3.2.3 Chemicals, paints or solvents
3.2.4 Lead-acid batteries
3.2.5 Light bulbs

From time-to-time, a load of materials may contain an example of the above materials. Upon receipt and recognition, Re-Teck will act quickly to inform the shipping party of the infraction and agree upon the next steps. Storage time will be kept to the minimum. As required by all federal and or local regulation(s), the disposal of these material will be performed by licensed agencies.

Bijlage 2

Overview of waste and Processing route

1 Waste

1.1 Re-teck receive discarded electronic equipment from different client's location. This equipment includes mobile devices such as mobile phones, music players, tablets, laptops, e-readers etc.

Since this is concerned with discarded electrical and electronic equipment, Re-teck also processing for a certificate of WEEELABEX. The table below lists the Eural codes that Re-teck applies with the associated description and global processing route.
Table 1, listing of Eural codes

Type Of Waste	Eural Code	Description	Processing
Electronics apparatus (like Mobile phones, MP3, tablet, laptop, PC)	160213* 160214 160215* 160216 200136	Faulty and discarded electrical and electronic equipment and components with / without hazardous components	In accordance with Activities Decree; sector plan 71 (by recognized processor, minimum standard is recycling of parts / materials or other useful application)
Batteries and charger	160605 200133* 200134	Other batteries and accumulators Urban waste; batteries	In accordance with Activities Decree; sector plan 13 (by authorized processor, minimum standard is the separating liquids and acids followed by recycling)
Connectors loose cords and cables	170411c	Cables do not fall under 170410	In accordance with Activities Decree; sector plan 14 (by recognized processing companies) ker; minimum standard is separate in a metal fraction, a plastic fraction and a residual fraction, followed by recycling the metal and the plastic fraction and 'other useful

			application ')

2 Contamination

Electronic waste Re-teck deals with may contain concentrations of toxic heavy metals or other metals including cadmium, lead, nickel, mercury, manganese, lithium, zinc, arsenic, antimony, beryllium, and copper.

Metals such as these are considered as:

- Persistent (ie don't degrade in the environment)

- Bioaccumulative (ie build up in fatty tissue so can reach toxic levels over time)

If any of these metals are allowed to leak into the environment, e.g. in a landfill when NiCd battery cases rupture or corrode, in significant quantities, they may leach into the water courses or contaminate the soil. Metals build up in the soil and they can then enter the food chain and in sufficient concentrations may cause health problems.

Chemicals such as these are associated with a range of adverse human health effects, including damage to the nervous system, reproductive and developmental problems, cancer and genetic impacts.

Cadmium for example is considered as the 7th most dangerous substance known to man. It is a toxic heavy metal that can harm humans and animals that ingest it. It is also carcinogenic.

The health effects of lead poisoning are well known. If lead is absorbed into the bloodstream in sufficient quantities it will cause serious liver and kidney damage in adults and neurological damage in children.

Nickel and mercury are toxic and are classed as hazardous substance. Although Li-Ion batteries are free of heavy metals (lithium has a low atomic number), lithium's high degree of chemical activity can create environmental problems. When exposed to water, which is present in most landfills, the metal can burn, causing underground fires that are difficult to extinguish

Landfill is not sustainable. Dumping mobile devices creates long term pollution risk to the environment. We at the Re-teck Reverse supply chain management Program believe that recycling mobile devices is the only sensible and conscientious alternative. We encourage everyone to take the social responsibility in making recycling a benefit for everyone by protecting the environment in which we live and work.

3 Processing Route

CUSTOMER ARRANGE THE DELIVERY OR Re-Teck PICKUP THE GOODS

- Re-Teck coordinates with each customer to arrange the logistics to transport materials to our facility
- Re-Teck and the customer utilize local logistics providers or Re-Teck-owned and operated vehicles
- From time-to-time, certain customer requirements must be met during transport including sealing the truck with serialized seals, non-stop transport and no co-mingling of customer’s materials with another customer’s materials
- All goods are transported according to all federal or local regulations

Re-Teck RECEIVES MATERIALS / TAKE PICS BEFORE UNLOADING

- Materials are delivered to the Re-Teck facility and received according to Re-Teck security and customer-specific processes which may include
  - Verifying of the driver’s identification and accompanying paperwork
  - Photographing the serialized truck seal before removal
  - Verifying the truck’s contents against the accompanying paperwork
  - Documenting any known discrepancies
  - Communications with the customer regarding discrepancies and resolutions

MEASURE WEIGHTS OF PALLETS AND TAKE PICTUTES WHILE WEIGHING

- All pallets are removed from the truck and weighed
  - This is the second step in verifying the contents of the truck
  - Weights are documented as part of mass balance reporting, see FINAL REPORTING
  - Discrepancies are reported to customers and resolutions are finalized
- Photographs of each pallet are taken as part of our receiving report
  - Photographs are provided to our customers
  - Photographs provide a basis for future reporting and discussion
- Materials are stored prior to next steps in the process
  - Storage assures each truck load is independently processed
- Materials are sorted as a complete truckload, independent of each other

SORTING

- Each pallet of materials is sorted in the first step of the disassembly process
- Materials are sorted and processed according to customer requirements

- Sorting categories may include
    - Whole units by type – e.g. mobile phone, computer
    - Intellectual Property (“IP”) revelatory whole units and components
    - Non-IP-revelatory materials
    - Ferrous and non-ferrous metals
    - Packing and packaging materials
    - Plastics

DATA SANITIZATION / DATA ERASURE

- Based on customer requirements, whole units which include mechanical or solid state (SSD) storage are wiped / cleaned of data
- Re-Teck employs proprietary, state of the art software

MANUAL DISSASEMBLY

- Highly-trained employees disassemble whole units in accordance with customer-specific, contracted statements of work
    - When possible, parts harvesting and reuse of the materials takes precedent
- Care is taken to sort all components removed from the devices
    - Li-ion batteries are properly prepared for storage and shipment to licensed downstream processors
    - Other components are prepared for further processing, resale or shipment to licensed downstream processors
    - Sorting assures clean streams of material are presented to downstream vendors or placed in the shredder

MECHANICAL SHREDDING

- In accordance with customer-specific, contracted statements of work and after manual disassembly, certain components are mechanically shredded to eliminate IP and provide size reduction for packing and shipment to licensed downstream vendors
- Shredding is performed by proprietary, self-contained machinery engineered and built to perform this specific function
    - Shredder operation is limited to specific, trained employees
- Clean material streams prepared in the Manual Disassembly process are shredded independently and stored, retaining the purity of each stream, maximizing value and minimizing further processing
- Shredder output is sold into the manufacturing stream for production of new products
- Other customer requirements eliminate shredding
    - Circuit boards containing IP-revelatory chips are drilled to eliminate reuse as-is
    - Circuit boards are sold to downstream vendors for smelting and precious metals recovery

FINAL REPORTING

At the end of processing, Re-Teck provides a Certificate of Destruction (“COD”) to the customer for each load processed. The COD is generally accompanied by other reports including a mass balance which provides the combined weight of all materials received (inbound), sorted (packing and packaging) and processed (shredded and sold to licensed downstream vendors). The mass balance is compared to the receiving weight to provide assurance that all material received is accounted for during processing.

WHAT WE DO NOT PROCESS

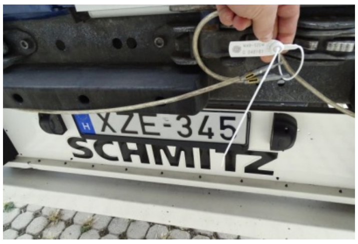
- Re-Teck does not accept and will not process the following materials
    - Materials contaminated with chemical and biological agents
    - Cathode Ray Tubes in any condition
    - Chemicals, paints or solvents
    - Lead-acid batteries
    - Light bulbs

From time-to-time, a load of materials may contain an example of the above materials. Upon receipt and recognition, Re-Teck will act quickly to inform the shipping party of the infraction and agree upon the next steps. Storage time will be kept to the minimum. As required by all federal and or local regulation(s), the disposal of these material will be performed by licensed agencies.

Bijlage 3

Receiving of material-In Control

- Accompanying documents (Delivery note, CMR, packing list) brought to the Operations Supervisor (OS).
- Before the truck or Container is opened photographs must be taken of the closed vehicle or container. If the vehicle is sealed then a photo is taken of the unbroken seal where the number can be clearly seen. The registration numbers of the truck and trailer or container number are also photographed.



- The truck /Container only then is opened, but before unloading, 2 – 3 more photos are taken from behind and wide diagonal. Should any pallets be damaged (packaging or physical damage), these are photographed also!

- Once unloading commences, each pallet is weighed on a calibrated scale and recorded in the Delivery Inbound Confirmation Documents (DIC). This document is saved to our network *Production/Delivery inbound control/Huawei/country/batchNr./DIC_XX-HUW-101-000x-jjmmtt* and can be found at this location for reference. Each pallet receives an individual number then weighed and photographed on the pallet scale. Weighed pallets are then booked from the Inbound area to the Sorting area. Pallets with damage are booked into the Quarantine area waiting on clarification.

- When a batch is booked from one warehouse location to another, 2 -3 photos are made in their respective locations.(Goods In , Quarantine etc.)

- Once all pallets have been weighed, DIC needs to be printed twice and handed to th OS.
- Drivers documents are completed by the OS and handed over to the driver.

INTERNAL AUDIT PROCEDURE

Bijlage 4

1.0 Goal

1.1 Establish and maintain an internal audit procedure, including procedures for planning, execution, reporting and follow up.

1.2 Purpose of Initiating an Internal Audit Procedure

- Verify that activities and relevant results are in compliance with the arrangement
- Assure the effectiveness of the management system
- Ensure that the management is in compliance with the quality, environmental and occupational health and safety.
- Ensure that standards such as ISO 9001:2015, ISO 14001:2015, OHSAS 18001:2007, R2:2013 and RIOS:2006 are complied.

2.0 Scope

2.1 Applicable to the internal auditing of integrated management systems (ISO 9001:2015, ISO 14001:2015, OHSAS 18001:2007, R2:2013 and RIOS:2006).

3.0 Responsibilities

3.1 Management representative is responsible for the monitoring and execution of internal audit.

3.2 Deputy management representative is responsible for monitoring internal audit as a delegated representative of the management.

3.3 Internal auditor will be responsible for the execution of the process.

4.0 Procedures

4.1 <u>Planning Internal Audit Procedures</u>

4.1.1 Management representative is responsible for creating internal audit teams to execute the internal audit procedures. The internal auditors should be trained as internal auditor of ISO 9001:2015, ISO 14001:2015, OHSAS 18001:2007, R2:2013 and RIOS:2006 standards and not be involved in the scope of work which his/her audit area is concerned.

4.1.2 Deputy management representative is responsible for the planning, co-ordination and implementation of internal audit procedures. The plan must be developed in accordance with the situation and level of importance of the auditee, and carried out at least once a year.

4.1.3 Internal auditors from each department should agree with the auditee on the audit period, and advise the deputy management representative accordingly, to compile an《Internal Audit Planning》.

4.1.4 Deputy management representative should develop an《Audit Document List》and《Non Conformity from Last External Audit》for every audit activity.

✧ Each Internal audit team member is responsible for auditing an area which does not belong to his/her own scope of work.

✧ Internal audit activities should be carried out in accordance with《Internal Audit Planning》,《Audit Document List》and《Non Conformity from Last External Audit》.

✧ Follow up with non-conformities in previous《Internal Audit Report》and《Corrective Action Report》from the last calendar year.

4.1.5 The《Internal Audit Planning》,《Audit Document List》and《Non Conformity from Last External Audit》should be disseminated to audited departments to ensure that the audit activity can be carried out smoothly.

4.1.6 Management representative and / or internal auditor is responsible for preparing the《Integrated Internal Audit Checklist》.

4.2 <u>Executing Internal Audit Procedures</u>

4.2.1 Iinternal audits should be carried out according to pre-planned《Internal Audit Planning》,《Audit Document List》and《Non Conformity from Last External Audit》.

4.2.2 Internal auditors is responsible to carry out audits according to requirements of《Integrated Internal Audit Checklist》, Integrated Management Handbook, Procedures Handbook, Working Guidelines, and standards of ISO 9001:2015, ISO 14001:2015, OHSAS 18001:2007, R2:2013 and RIOS:2006. Audit should be done through examining relevant information records, by interview and by observation of operations, in order to ensure a compliance to the requirements of the management system. All objective evidences observed through the audit process must be recorded in the《Integrated Internal Audit Checklist》.

4.2.3 Verify whether substandard items observed in previous《Audit Report》were resolved, including its implementation and effectiveness.

4.3 <u>Reporting on Audit Report</u>

4.3.1 If substandard items are observed, the internal auditor should make a record and follow up on the issue.

4.3.2 Upon completion of the audit process, management representative and the internal auditor should compile all items observed to be substandard and draft an《Internal Audit Report》.

✧ Number of items classified as substandard

✧ Audit record of substandard items observed in previous audit

4.3.3 Upon the completion of the audit activity, management representative and the internal auditor and the department head of the audited department will meet for a closing.

4.3.4 The purpose of the closing meeting is to:

✧ Report and identify audit results

✧ Issue an《Internal Audit Report》for relevant persons for follow up.

4.3.5 The《Internal Audit Report》,《Integrated Internal Audit Checklist》and other documents should be submitted to management representative for record and planning for follow up measures.

4.4 Follow Up on Internal Audit Report Procedures

4.4.1 Internal Audit results, including items categorized as substandard, should be detailed in the《Internal Audit Report》. Relevant persons should execute rectification and prevention measures indicated in the《Internal Audit Report》.

4.4.2 Management representative should review items categorized as substandard in the《Internal Audit Report》, to ensure that they are verified and will be followed up with.

4.4.3 Internal audit results, including the verification of whether substandard items identified in previous audits were resolved, methods of resolving and its effectiveness, is required to be reported in the Management Review Meeting every year. The management representative is responsible for reporting to the Directors.

5.0 References

5.1 Integrated Management Handbook

5.3 Management Review Procedures

6.0 Record

6.1 Internal Audit Planning

6.2 Audit Document List

6.3 Non Conformity from Last External Audit

6.4 Integrated Internal Audit Checklist

6.5 Internal Audit Report

CORRECTIVE ACTIONS PROCEDURE

1.0 Goal

1.1 Establish and maintain rectification and prevention measure procedures to ensure:

- An effective execution of the established rectification measures
- Develop complaint handling procedures and reporting of substandard situations
- Investigation on causes for substandard situations
- Record of all measures in rectifying and preventing substandardness
- Review feasibility of current rectification measures
- Review and analyse potential for substandard scenarios

2.0 Scope

2.1 When an item is observed to be substandard, procedures should be followed in order to establish, implement, maintain, review and record relevant rectification measures.

3.0 Responsibilities

3.1 Various department managers should:

- Investigate and review external and internal complaints within its jurisdiction
- Develop rectification measures and put in record of the “Rectification Measure Report”
- Monitor the execution of rectification measures.

3.2 Responsibilities of the management representative includes:

- Review the effectiveness of suggested rectification measures
- Monitor the execution of rectification measures

4.0 Procedures

4.1 Definition of non-conformity (confirm the need for corrective action)

In case of (1) external audits, (2) regular environmental monitoring in workplace (air quality monitoring and dark smoke test), (3) non-compliance in monthly environmental and safety walkthrough inspection for 4 times consecutively, or (4) receipt of external compliants about the non compliance in the quality, environmental, occupational health and safety management system that cannot fulfil any of the following requirement, the non compliance is defined as non conformity or potential non conformity:

- Customer requirements
- Legal requirements

- ✧ ISO9001:2015, ISO14001:2015, OHSAS18001:2007, R2:2013 and RIOS:2006 standard requirements

When discovering non conformity and potential non conformity, the department or personnel should request the relevant department to handle the problem in accordance with 《Corrective Actions Procedure》.

4.2 The Mechanism of assessment for substandard items

4.2.1 Handling external complaints on substandard items

- ✧ In accordance with the 《Internal and External Communication Working Instruction》, upon receipt of external complaints, staff must report to their direct supervisor or manager, who is required to communicate with the source of the complaint via the staff or in person to understand content of complaint.
- ✧ Should the supervisor or manager decide that the complaint is valid, he/she should investigate in the cause of the substandard item in person or via a relevant department, in order to develop and execute the appropriate rectification measures.
- ✧ Manager and Department in charge of the investigation should follow up with and review the execution of rectification measures, to ensure that the complaint has been rectified and properly handled
- ✧ If the rectification and prevention measures are ineffective, department in-charge or the manager will have to seek for advice from the management representative for alternative measures.

4.2.2 Handling substandard items observed in daily operations, internal meetings or external assessment

- ✧ If substandard items are observed in daily operations, internal meetings or external assessments, relevant department in charge should investigate in the cause for the substandard item.
- ✧ Department in charge is responsible for suggesting targeted rectification measures, which may be delegated to relevant persons for follow up.

4.2.3 Investigating the root cause of substandard item

4.2.3.1 The relevant department should collect the following information when investigating the root cause(s) of substandard item

- ✧ Onsite walkthrough inspection
- ✧ Collect data of personnel, machineries, objects, methodologies, environment, potential health and safety risks, potential environmental impacts and any other data related to the substandard item
- ✧ Interview with relevant personnel

4.2.3.2 Consolidate and analyze the data collect from the previous step

4.2.3.3 Conclude analytical result to find out the root cause(s) of substandard item

4.2.4 Verifying the need for implementing corrective measures

After conducting root causes analysis, the relevant department should draft the corrective measures, and evaluate the measures according to the following criteria:

✧ The effectiveness of eradicating the non-conformity

✧ The feasibility and easiness of implementing the measures (may consider the cost and scope of influence including department, environment and behavioral changes etc.

The relevant department should firstly implement the most feasible, the easiest and the most effective measure. And the department should implement the rest of the corrective measures with the available resources

4.2.5 Record and Verify the Implementation Progress and Effectiveness of Corrective Measures

✧ Department observing the substandard situation or the department that communicated with the complainant should fill in the《Corrective Action Report》, describing how substandard items were observed and other relevant details. Departments responsible for the substandard situation should be responsible for investigating the cause for substandard situation, and should suggest rectification and prevention measures, and include the reason, analysis, suggestions for rectification measures in the designated area. The report should then be reviewed by the management representative.

✧ Upon completion of corrective measures, the issuing department manager, executional department manager and management representative will review the implementation progress and effectiveness of the measures through the following channels:

➢ Review of existing operational situation

➢ Delegation of an internal assessor to monitor the situation

➢ Diliberation during the Management Review Meeting

✧ All three parties should ensure that substandard items were properly rectified and handled prior to signing a closure report.

✧ Management representative is responsible for closing the case with a closure report.

5.0 Reference

5.1 Internal and External Communication Working Instruction

6.0 Record

6.1 Corrective Action Report

Bijlage 6

Re-Teck
REVERSE SUPPLY CHAIN MANAGEMENT

IT-Security Concept

LTG Technology Services Europe BV
Grenssteen 33, Breda 4815 PP
Netherlands

Contents

1 Introduction

This IT policy is intended to support the Company's actions to protect its equipment and protect (personal) information from unauthorized third party or unauthorized disclosure.

2 Scope

This IT policy applies to all employees of the company. External persons who regularly work in the company are required to abide by the provisions of this policy.

3 Compliance with Legislation

When using the IT systems and applications in the company, the employees must comply with the applicable data protection and data security regulations as well as company regulations. If employees are unsure as to whether and to what extent legislation or company regulations must be complied with, they should contact their supervisor for clarification.

4 Structure

The following is a list of all the risks relevant to business activities. The presentation of the dangers and corresponding measures takes place in the form:

1. **Threats Identification**

   1.1 Description of threats

   1.2 Measure

   1.3 Procedure in case of emergency

5 Lightining (High Voltage)

5.1 Lightening

5.1.1 Description of threats

A lightning strike in the commercial building can destroy electrical appliances.

5.1.2 Measures

- Existing and tested building lightning protection system
- Obligatory security for home wiring
- Power strips with appropriate overvoltage protection

5.1.3 Procedure in case of emergency

In case of emergency, all systems must be tested for functionality. Strips damaged by the lightning strike must be replaced immediately.

If a power failure occurs, proceed as described in case of power failure.

5.2 Power Failure

5.2.1 Description of threats

A power failure in the commercial building or individual parts of the building can restrict business operations.

5.2.2 Measures

The alarm system and the electronic access system function by a built-in emergency power supply even in the event of a power failure. The employees are equipped with laptops that enable further work even without an external power source.

5.2.3 Procedure in case of emergency

- Locate the fault; if possible fix it yourself otherwise contact electrician (Elektrotechnik Bedrijf)
- In the event of total failure: Contact the electricity supplier (Engie)
- Battery operated devices (notebooks): save open files & close programs
- Park electrically operated implements (forklifts) in their parking positions so as not to obstruct emergency exits
- electrically operated gates, roof hatch, entrance doors in case of prolonged power failure, if possible operate manually
- Inform Security company alarm center about power failure

When power is restored, make sure all systems are working properly again..

5.3 High Temperature / Humidity

5.3.1 Description of threats

IT equipment must not be used under conditions it is not intended for (for example overheating the IT room). This can lead to the destruction of the devices.

5.3.2 Measures

- Currently, the IT room is adequately ventilated, so that from today's perspective air conditioning of the IT room can be dispensed with.
- Regular temperature control by entering the IT room
- All IT equipment may only be operated under the intended climatic conditions

5.3.3 Procedure in case of emergency

In the event of deviations from the intended climatic conditions, the intended conditions must be established (for example, opening the door of the IT room) or, if this is not sufficient, switch off the appliances.

5.4 Dust / Contamination

5.4.1 Description of threats

Soiling of IT equipment (especially in the production hall) can lead to destruction of the equipment or causing fire (for example due to clogged fans).

5.4.2 Measures

- Suitable storage of portable PCs for mobile use
- Entrance to storage cabinet in the production hall
- Obligation of users to take appropriate measures against pollution
- If possible, do not use IT equipment in heavily dusty or otherwise unsuitable environments
- See also Impermissible temperature / humidity

5.4.3 Procedure in case of emergency

Employees are required to remove contamination immediately or to ask an IT representative for help. Dirty equipment should be switched off or not or only used in a suitable environment.

5.5 Failure of external Network

5.5.1 Description of threats

Failure of the internet connection. Power failures are already covered by power failure.

A failure of the Internet connection can limit business operations..

5.5.2 Measure

To secure the devices (Modem & Switch), the Internet service provider uses a combination of technologies that prevent us from accessing the devices.

In addition, all devices are regularly updated by the internet provider to the latest software version. The well-rehearsed software version is the current version recommended by Cisco.

All network elements are permanently monitored by the monitoring system.

If a failure is detected, external technicians will proactively notify 24x7 and immediately take care of the analysis of the reported condition.

The central network management system of the internet provider holds all events that are generated by the network devices at all network levels. All events are collected, automatically analyzed for abnormalities and archived for later analysis.

For emergencies there is internally a mobile radio router, as well as a USB portable radio modem.

The procedure for starting / using the router is to be carried out by the IT manager and found under "R: \ RTA_IT \ Arbeitsanstellungen_IT \ Ausfall_Internet.docx".

5.5.3 Procedure in case of emergency

IT staff need to know the current status of the Internet service provider (MassResponse +43 1 270 28 25). The business processes can be continued to a lesser extent without internet.

6 Threat (Organisation Lapses)

6.1 Unauthorised Entry

6.1.1 Description of threats

Employees or external persons have access to rooms for which they are not authorized. This can lead to intentional or unknowable disruptions of the IT infrastructure.

6.1.2 Measure

- Access to security-relevant premises is regulated by the local management.
- Access is only possible with the help of keys or electronic keys.
- Security-relevant rooms are generally to be blocked.
- After completion of the work and in the absence of these rooms are to be blocked again.
- Doors and gates to the outside must always be kept closed when not in use.
- Outside the operating hours, unauthorized access by an alarm system is prevented.
- If unauthorized access is detected by an employee, they must immediately report it to their supervisor.

6.1.3 Procedure in casse of emergency

If an unauthorized access occurs, the incident must be reported to the management, an analysis made and appropriate precautions are taken.

6.2 Unauthorised Access

6.2.1 Description of threats

Employees or external persons have access to IT equipment for which they have no authorization. This can lead to intentional or unknowable disruptions of the IT infrastructure.

6.2.2 Measures

- Employees are required to keep the IT equipment provided to them safely.
- Access rights are granted by the IT officer in coordination with the management (GF sends a written request by e-mail for extension of access rights to IT managers - path including information regarding read and write rights)
- Password protection for IT equipment
- Automatic screen locks on servers
- Control of password properties (length, special characters, ...)
  o End users are responsible for choosing safe passwords
  o Server passwords must:
    □Be at least 10 characters long
    □Special characters, numbers, uppercase and lowercase letters included
- Confidentiality of passwords
- Passwords may not be publicly accessible in writing (for example, notices in the workplace)
  o Employees must never forward their passwords to unauthorized persons (internal / external)
  o Passing of passwords requires the permission of the management
- Suitable physical and logical segmentation of the network
  o Separation of alarm system and internal network
- User profiles to restrict usage
- Block and / or delete unneeded user accounts
- Restricting access to files and directories on the file server
- Access to the file server from outside the company network is only possible via an encrypted HTTPS connection.
- If unauthorized access is detected by an employee, they must immediately report it to their superviso.

6.2.3 Procedure in case of emergency

If unauthorized access to data occurs, the management must be informed, the incident analyzed and appropriate action taken.

See also NAID post-incident analysis.

In addition, proceed as described in Confidentiality of data (procedure in case of emergency).

6.3 Insufficient maintenance

6.3.1 Description of threats

The maintenance of IT equipment is not performed regularly or properly. This can lead to operational degradation and make the equipment vulnerable to other hazards (e.g., computer viruses).

6.3.2 Measures

- The IT staff are responsible for:
  - o Regular checking of the protocols generated by network equipment
  - o the correction of errors resulting from protocols
  - o Regular updating of the device firmware for network equipment
  - o the backup of the device configuration before updating the firmware
  - o the perfect condition of the network equipment
  - o the replacement of disabled network equipment
- In addition, they must ensure the following on each end-user device:
  - o Automatic update of Windows operating systems by Windows Update
  - o automatic update of anti-virus software

6.3.3 Procedure in case of emergency

If an employee finds out that IT equipment is not properly maintained, they must report it to an IT representative. This person has to react within a week to the message..

6.4 Insufficient Documentation

6.4.1 Description of threats

Missing or outdated documentation can affect the operation of IT equipment and make maintenance difficult..

6.4.2 Measures

- Documentation of the system configuration (device directory)
- Documentation of authorized users and rights profiles
- Documentation of network components (network plan)
- Documentation of changes to an existing system
- Identification of the wiring
- Centralized administration of manuals on the file server
- IT staff are responsible for promptly adapting the associated documentation when the system changes (for example, if a network cable is permanently unplugged).

6.4.3 Procedure in case of emergency

If it turns out that the documentation does not match the actual situation, this documentation should be revised as soon as possible.

If no documentation exists, a meaningful documentation must be compiled as quickly as possible and made accessible to the employees concerned.

6.5 Confidentiality of Data

6.5.1 Description of threats

Company‘s data is an advantage for competitors. If company‘s data, or data from customers are forwarded to unauthorized persons this can lead to business loss.

6.5.2 Measure

• Written commitment of employees to confidential treatment of all data under the employment contract
• Indication of the confidentiality in the e-mail signature
• Storage of data carriers of customers in restricted areas
• Regulated procedure when new employees join (see procedure when new employees join)
• Regulated procedure when leaving employees (see procedure when leaving an employee)
• If the unauthorized disclosure of company data or data of a customer is noticed or suspected by an employee, he must immediately report this to his supervisor.
• Data carrier is securely destroyed by IT managers (Data Sanitization). Afterwards, the creation of a "Certificate of Destruction"

6.5.3 Procedure in case of emergency

If company data are passed on unauthorized by an employee, the person concerned must expect consequences under employment law.

If company data is read out by external persons ("hacking"), the IT department must immediately take appropriate measures to prevent further attacks.

If data are passed on by customers without authorization or "hacked" or if there is a suspicion, the procedure is the same as for company data. In addition, the affected customers (in accordance with the NAID regulations) must be informed immediately upon discovery of the incident..

7 Threats (Technical problem)

7.1 Data Loss

7.1.1 Beschreibung der Gefahr

Company data can be lost due to a defect in the storage medium.

7.1.2 Measures

- All quality-relevant data is stored centrally on a server.This data may not be stored on the workstations alone.

- The server has both mirrored hard drives, on the other hand, a backup via an external hard drive, which once a week in at least 3 generations, the movement data are backed up, and once a month in at least 12 generations.
- In addition, changes to the transaction data from the server are stored twice per hour as a backup copy to a defined drive in the network and thus kept in sync.
- The software for data deletion is provided by the Group and does not require data backup.
- IT staff are responsible for ensuring that these backups are complete and can be restored in the event of an emergency..

7.1.3 Procedure in case of emergency

An IT representative checks the affected device, repairs or replaces it, and restores the data to the backup.

The procedure for emergency operation is to be carried out by the IT manager and can be found under "R: \ RTNL_IT \ WI_IT \NAS.docx".

8 Threats (Human Error)

8.1 Unstructure Data management

8.1.1 Description of threats

An unstructured data storage complicates the daily work and the allocation of access rights and may lead to data leaks and conflicts between employees.

8.1.2 Measures

• Easy-to-understand folder structure on the file server
• Preventing changes to the basic folder structure (1st level)
• appropriate read / write permissions on directories to prevent intentional or accidental deletion, overwriting, etc.

8.1.3 Procedure in case of emergency

If data are stored unstructured despite the precautions, the read / write permissions of the affected files and directories must be adjusted.

If an adjustment of the read / write rights does not make sense, the employees concerned are informed again about the importance of structured data management. The data is brought into an acceptable structure by the "polluter" or an IT staff member.

8.2 Improper handling of IT-Equipment

8.2.1 Description of threats

Employees can unconsciously or intentionally use their IT equipment in ways that cause significant damage or other hazards.

8.2.2 Measures

Employees are required to:

- For questions about the use of the equipment, contact an IT manager
- Programs may only be installed by IT managers
- Use IT equipment only for operational purposes
- Store IT equipment in suitable climatic conditions
- Inform colleagues about correct handling when IT equipment is used improperly
- Never leave the laptop in the car or leave it unattended
- Only encrypted laptops may be taken out of the home (overview of encrypted laptops and passwords: R: \ IT_Support \ Inventar \ bitlocker_keys)
- Do not save company data locally on the laptop
- Always lock the laptop when leaving work (especially when teleworking)
- Company phones must be encrypted with screen lock / code
- Apps may only be installed in consultation with the person responsible for IT
- CDs with sensitive data are prohibited
- Only encrypted and password-protected USB sticks may be used
- Downloads are not allowed - Employees must contact IT managers
- Disconnect devices properly (not via the switch on the distributor plug!)

8.2.3 Procedure in case of emergency

If an employee does not comply with the requirements for the proper handling of IT equipment, he will be warned.

9 Threats (Intentional mishandling)

9.1 Unauthorised use

See unauthorised access.

9.2 Computer Virus and Malware

9.2.1 Description of threats

Different types of malware pose a threat to the confidentiality of data and the availability of IT equipment.

9.2.2 Measures

- Administrators must ensure that
  - new devices that are integrated directly into the corporate network, trusted and equipped with appropriate antivirus protection
  - Devices that are infected with malware are immediately removed from the network
  - programs to be installed are checked for trustworthiness
  - Current virus protection is installed and activated on all devices
  - Virus protection is updated regularly and performs regular scans
- Every user must ensure that
  - As soon as he suspects malware on his device, the device immediately disconnects from the network and informs an IT staff
- Secure configuration of network equipment
  - active firewalls
  - Password-protected access to settings
  - Port releases only to used ports
- E-mails are additionally checked by the virus protection of the mail provider

9.2.3 Procedure in case of emergency

If an employee suspects malware on a device, they must immediately disconnect it from the network and inform an IT staff. The IT department must immediately investigate the suspicion and take appropriate action for the rest of the company.

10 Procedure when a new employee join

1. Define access and access authorizations with management
2. Prepare keys, configure keycards
3. Set up user account on the laptop / PC
4. Set up user account on the file server
5. Prepare the phone
6. Activate e-mail address
7. Inform new employee about rights and duties
8. Change the default passwords by the new employee

11 Procedure of releasing an Employee

1. Collect keys, take back access cards
2. Take back laptop, PC, phone
3. Remove user account from laptop / PC
4. Deactivate / remove user account on the file server
5. Change the passwords that the employee has assigned
6. Reset the telephone if necessary
7. If necessary, set up forwarding for the telephone
8. Set up e-mail forwarding / initiate deletion of the e-mail account

12 NAID Post-Incident-Analysis

In the event of an incident that threatens the security of customer data, a post-incident analysis must be conducted within 14 days and approved by the management. The form can be found under "R: \ Templates \ Post_incident_analyse13022017.docx".

13 Glossary

Company Data	Data intended exclusively for Re-Teck
Internet-Service-Provider	Internet-provide (in our case KPN)
IT-Equipment	All electronics devices (Desktop-PCs, Server, Laptops, Smartphones, Router, Switches, etc.)
Customer Data	Data from customers on storage media intended for destruction
Netwerk-Equipment	Router, Switches

RESOURCE USAGE INSTRUCTIONS

Bijlage 7

1.0 Goal

1.1 Improve the efficiency of use of resources and reduce the waste of resources.

2.0 Scope

2.1 Applicable for resource usage in offices and warehouses, including resources such as water, electricity, paper and other consumable materials.

3.0 Responsibilities

3.1 Responsibilities of managers from each department :

- Use resources in accordance to the Working Instruction
- Supervise employees in their adherence to the Working Instruction in using resources

3.2 Responsibilities of management representative:

- Advocate conservation activities, encourage employees to effectively use resources and minimize wastage

4.0 Procedures

4.1 Water conservation

- Ensure taps are closed properly after use before leaving the premises
- If taps or pipes are found leaking, inform relevant persons for maintenance
- Avoid splashing of water to avoid wastage. If possible, recycle wastewater for other usage, such as floor cleaning
- If possible, use water saving sprinkling devices

4.2 Electricity conservation

- Consider energy conservation functions and automatic options when purchasing new equipment
- Regularly inspect and maintain existing equipment and facilities, such as clean filters of air conditioners on regular basis
- If there are abnormalities in the operation of the equipment, such as abnormal sounds, heat or smoke. Stop using the equipment and inform relevant department immediately to arrange maintenance

✧ During breaks or when not in use, turn off the machinery and equipment, such as computers, lights, projectors, forklifts, etc.; Other equipment that cannot be turned off, such as servers, should be clearly marked

✧ To reduce the unnecessary use of air-conditioning equipment. In the hot months (April to October), the room with air-conditioning temperature shall be maintained at 27 degrees or above (except the days with outdoor temperature is below 27 degrees)″ ; In colder months (November to March), all air-conditioning equipment shall be ceased to use the cooling mode when opened for ventilation systems. EHS department conducts monthly random inspection and record the inspection results in the《Environmental Inspection checklist》. If there are issues not to comply with the above rules, the the person in charge of temperature control are required to make correction immediately

4.3 Saving papers, ink, ink cartridges, toner and toner cartridges

✧ Employees should avoid printing documents; if printing is necessary, it also requires two-sided printing

✧ Employees should maintain and recycle waste papers with one side printing

✧ Employees have to return the spent ink cartridges and toner cartridges to suppliers for reuse if suppliers are able to do so; otherwise, employees have to pass the spent ink cartridges and toner cartridges to qualified downstream for recycling

4.4 Economize on the use of other materials

✧ Use reusable product, including tableware made up of tile, glass or metal and refillable stationeries etc., to avoid using one-off e.g. paper cups and plates, or over packing product

✧ If it is approved by customer, the business development department will inform the administrative department or warehouse, to take customers' goods for self-use; depending on the category and quantity of the goods, administration could distribute some goods to employees for personal use

✧ Set up recycling bins for recycling metal cans, plastic bottles, waste paper and plastic bags (for warehouses only), to recover those materials for recycling

✧ In project planning period, use of recyclable materials should be taken into account, such as using reusable metal parts instead of wood accessories

5.0 References

5.1 None

6.0 Record

6.1 Environmental Inspection Checklist

BATTERIES
DIFFERENTIATION AND STORAGE

Bijlage 8

- **Lithium batteries (Li-ion, Li-po)**
- **Non-Lithium batteries** (Lead, NiCd, NiMh)

Lithium Batteries

Identification:

Marking on the battery: „**Li-ion**“ or “**Li-po**“ respectively „**Lithium-Ion**, **Lithium Polymere**“.
Present in consumer electronics such as mobile phones, cameras, notebooks as well as in cordless screwdrivers, e-bikes and many more applications.

Attention:
Due to the high charging density lithium-ion batteries are highly fire hazardous. Mechanical damages of the battery, short-circuits of the contacts can cause spontaneous and violent fire. Lithium batteries therefore are never to be damaged with sharp or pointed items. Never short-circuit the contacts of the battery. Special storage in flame-retardend containers is required.

Sorting:

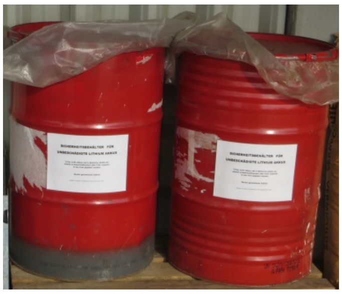
Visual control for damages and sorting into 2 categories:

1) **Undamaged lithium batteries**

No external damage perceivable. Not „inflated“.

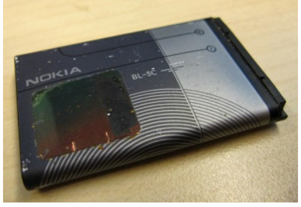
Put these batteries <u>individually</u> into plastic bags and store them in clamping ring barrels. Keep the barrels closed.

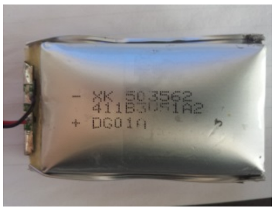
BATTERIES
DIFFERENTIATION AND STORAGE

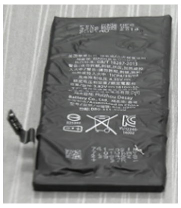


2) Damaged lithium batteries:

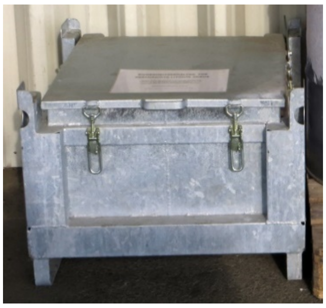
- Damaged housing (broken, deformed), strongly bent contacts
- Dismounted batteries for soldering assembly with exposed contacts or cable heads
- Battery is “inflated”







Put these batteries individually into plastic bags and store them in the metal box. Cover with special sand. Keep box always closed.

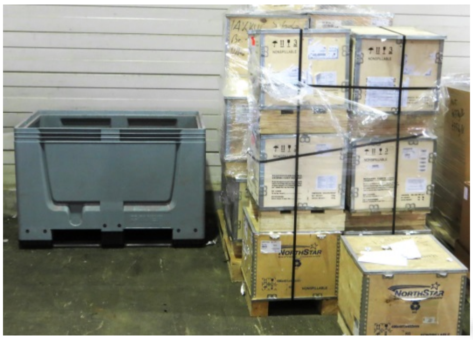


Non - Lithium Batteries

Identification: Marking on the battery: Lead (Pb), Nickel Cadmium (Ni-Cd), Nickel Metal Hydride (Ni-Mh)

Are separated by type and stored either in the original packing (wooden box) or in plastic containers sealed laterally and at the bottom (plastic paloxe, plastic box).

BATTERIES
DIFFERENTIATION AND STORAGE



Pallet box

Original packing – wooden box

Bijlage 9 HUAWEI

A. Receiving Process

1. Weighing

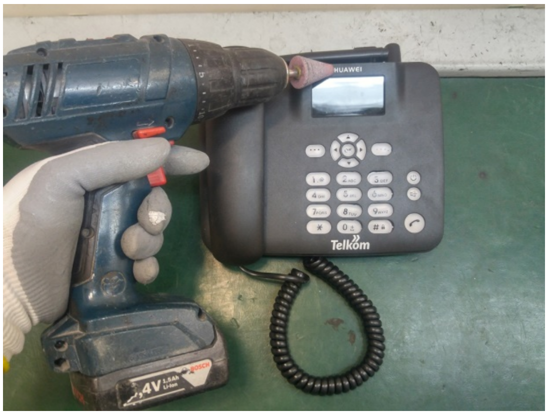
1. Weighing

2. Unpacking

2. Unpacking

3. Telephone Before Scrapped

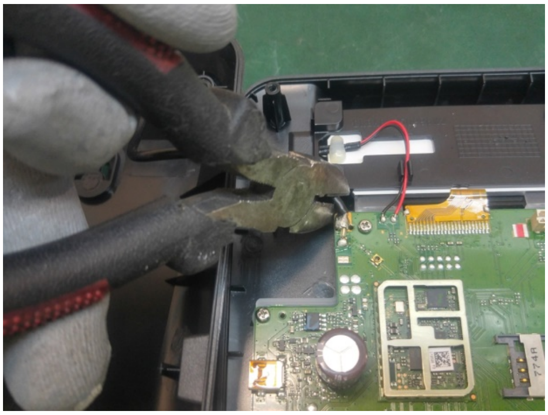
3. Removing Logo



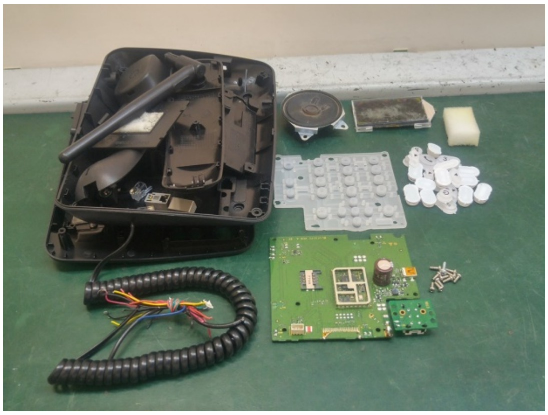
B. Disassembly Process

3. Unscrewing

4. Cutting Wire



5. Scrapped telephone

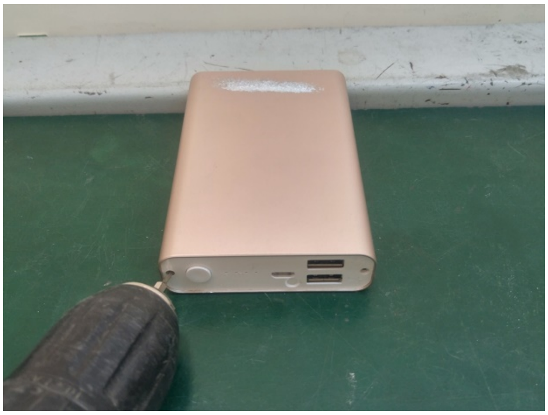


4. Power Bank 1 Before Scrapped

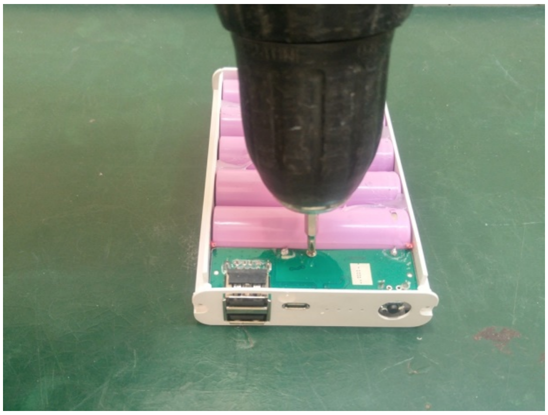
4. Removing Logo

B. Disassembly Process

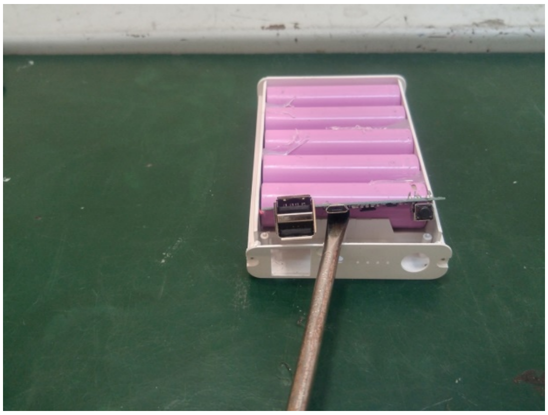
4. Unscrewing



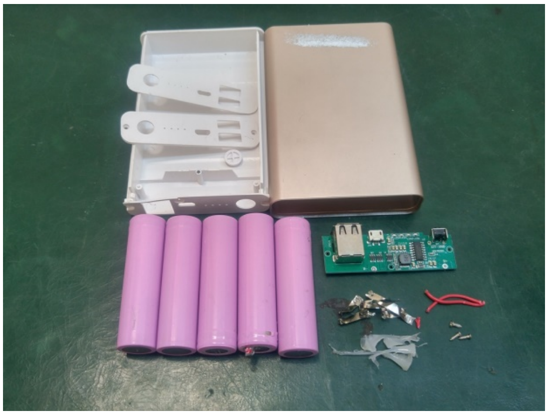
4. Removing PCB



4. Removing Battery

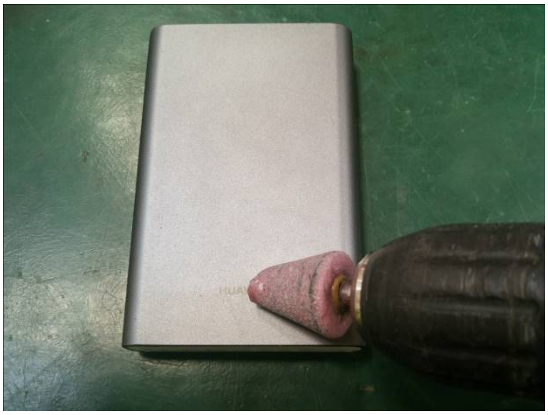


4. Scrapped Power Bank 1



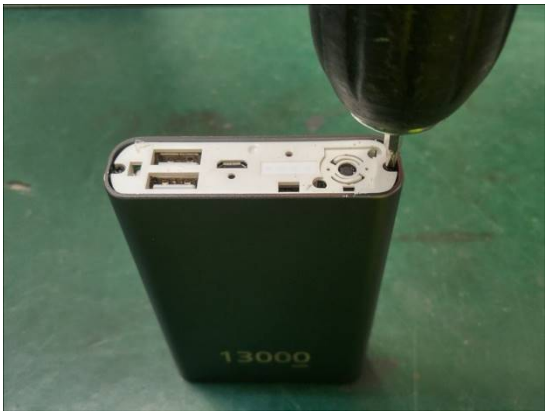
5. Power Bank 2 Before Scrapped

5. Removing Logo

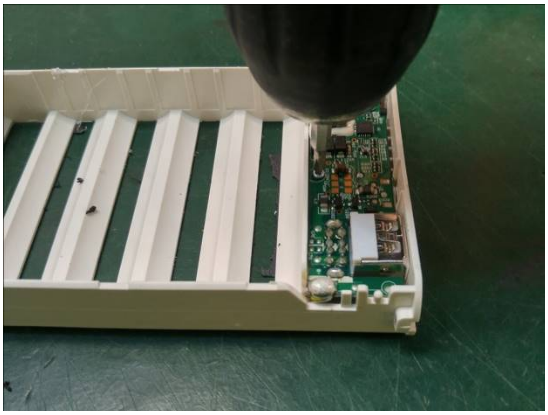


B. Disassembly Process

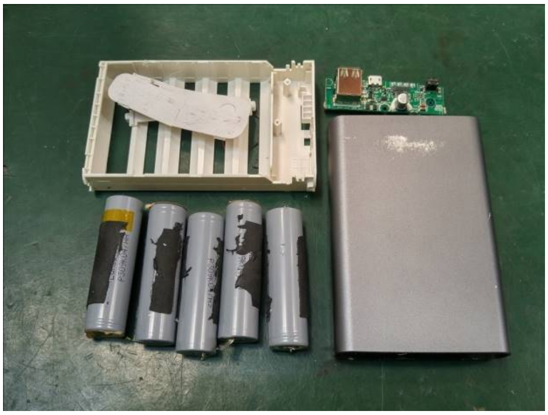
5. Unscrewing



5. Removing PCB

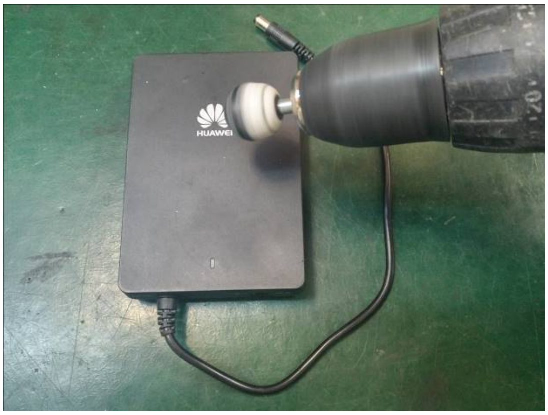


5. Scrapped Power Bank 2

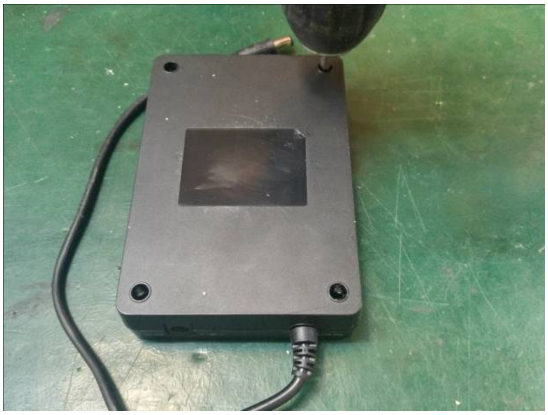


6. Backup Battery Before Scrapped

6. Removing Logo

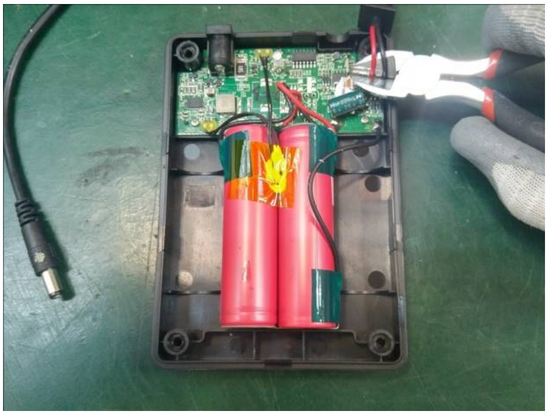


6. Unscrewing

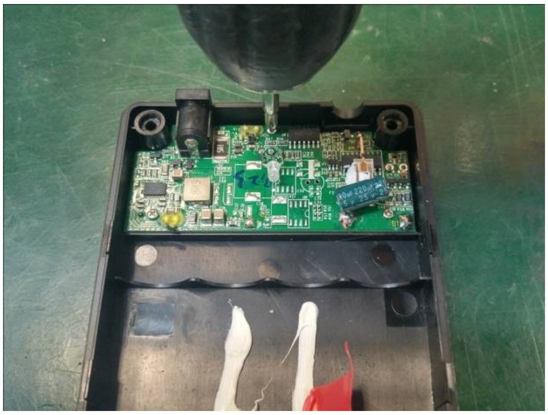


B. Disassmbly Process

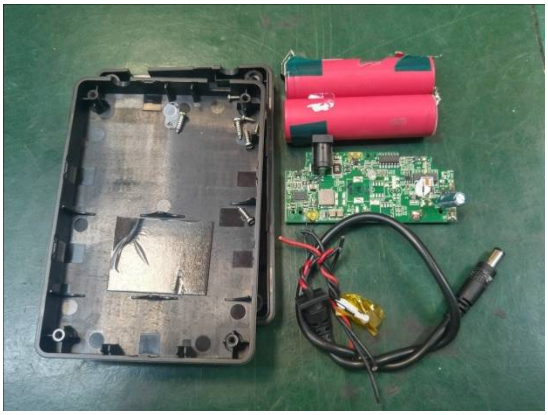
6. Cutting Wire



6. Removing PCB

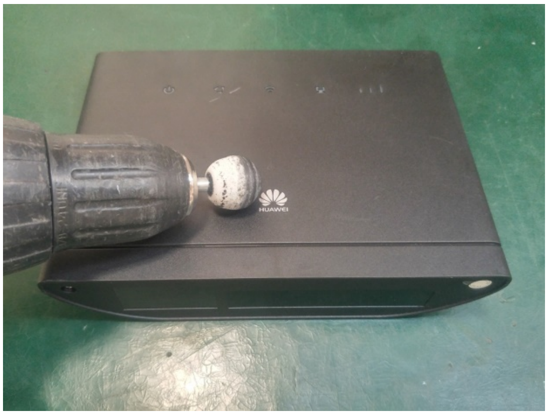


6. Scrapped Backup Battery

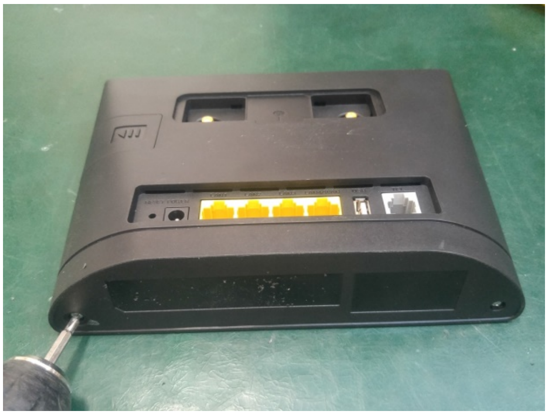


7. Router Before Scrapped

7. Removing Logo

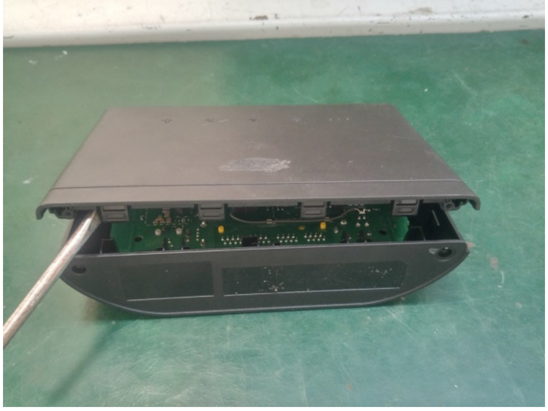


7. Unscrewing

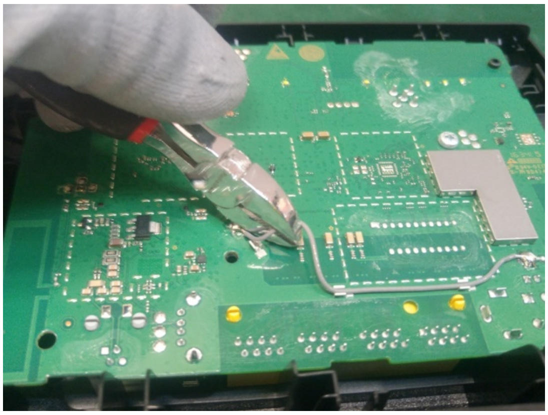


B. Disassembly Process

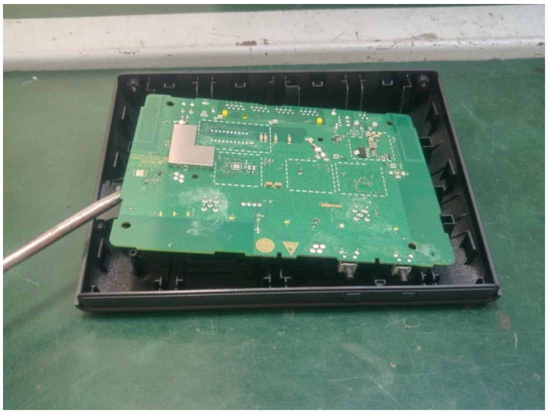
7. Dismantling



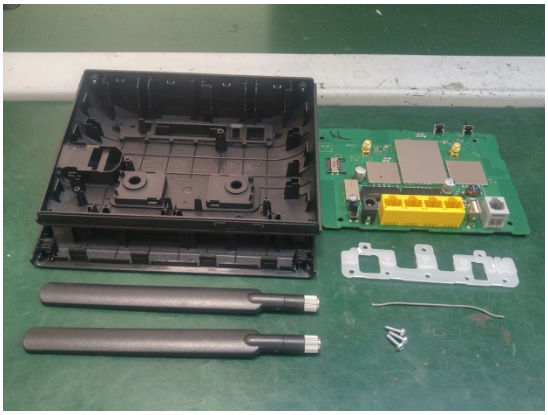
7. Cutting Wire



7. Removing PCB

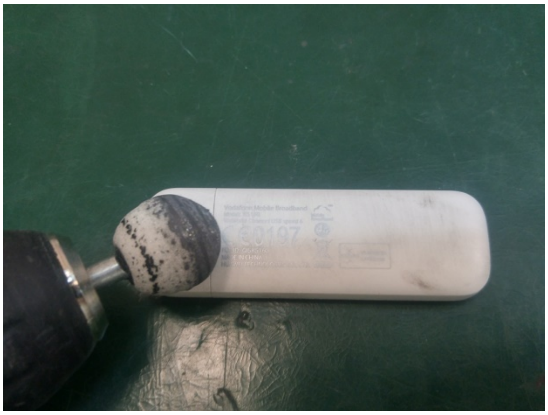


7. Scrapped Router



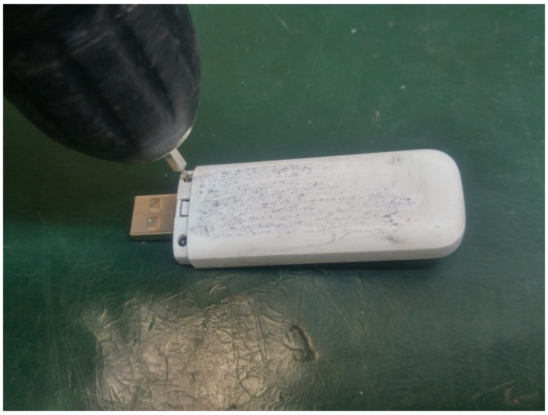
8. Wireless Broadband Before Scrapped

8. Removing Logo

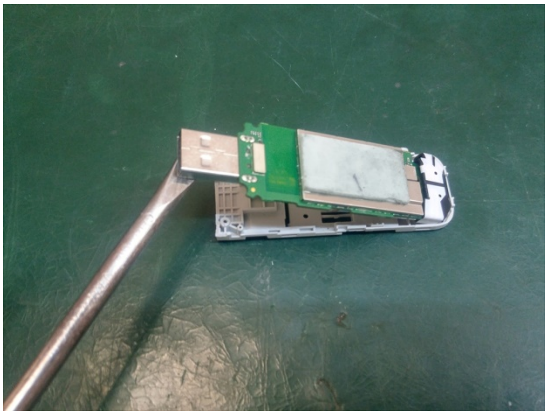


C. SortingProcess

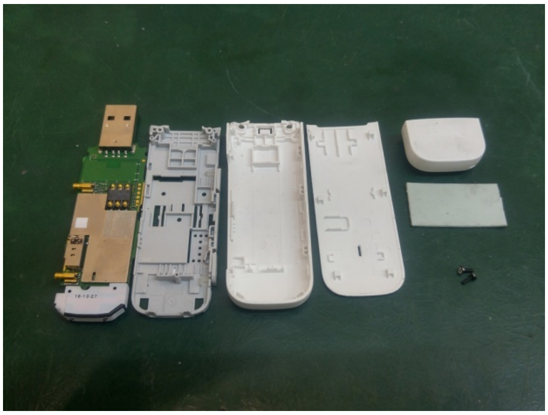
8. Unscrewing



8. Removing PCB

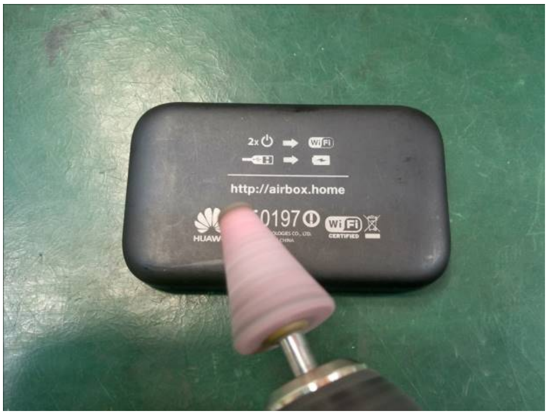


8. Scrapped Wireless Broadband

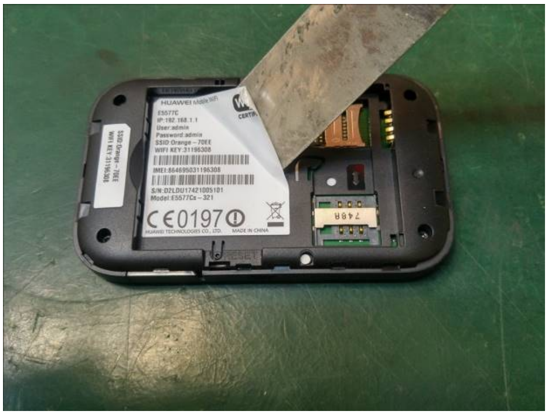


9. Pocket Wifi Before Scrapped

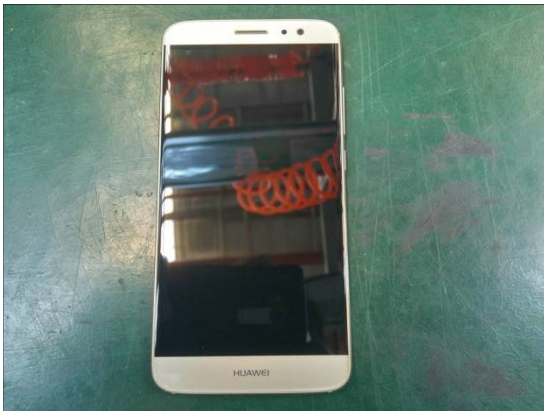
9. Removing Logo



9. Removing Label



C. Separating Process

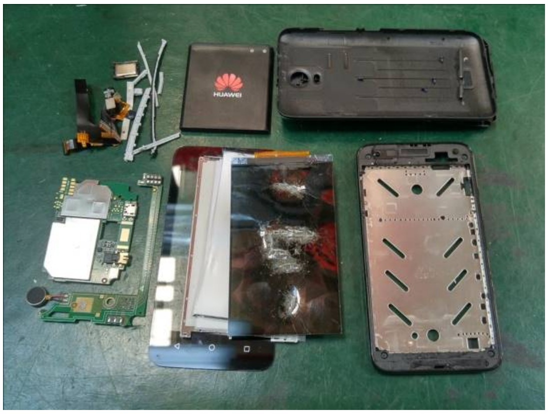


14. Mobile Phone 2 Before Scrapped

14. Removing Logo

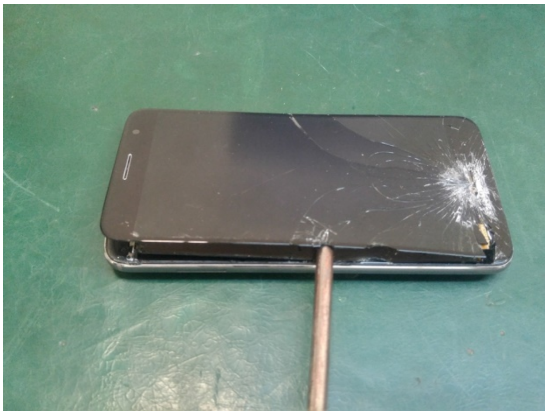
14. Unscrewing

14. Cutting Flex

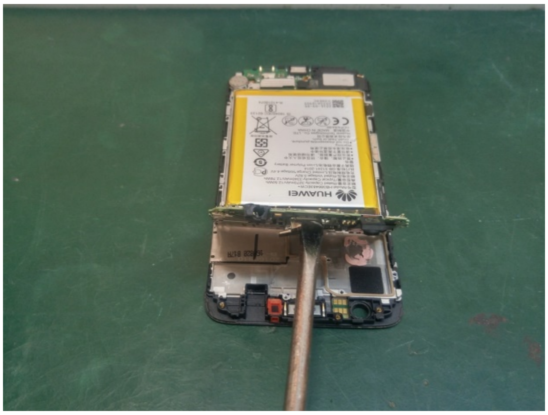


C. Separation Process

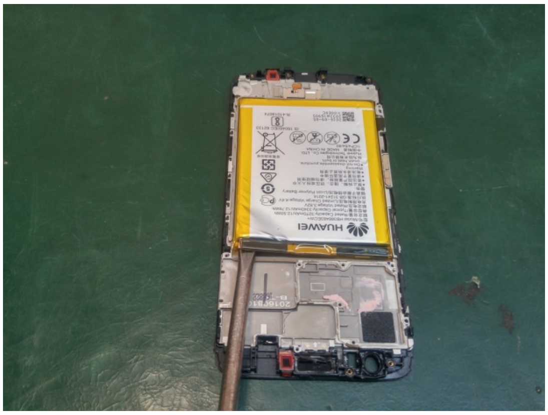
15. Dismantling



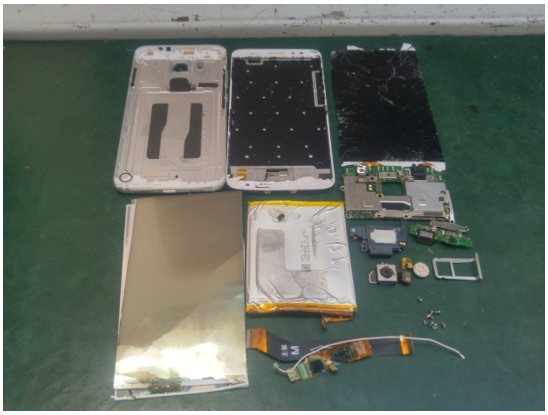
15. Removing PCB



15. Removing Battery

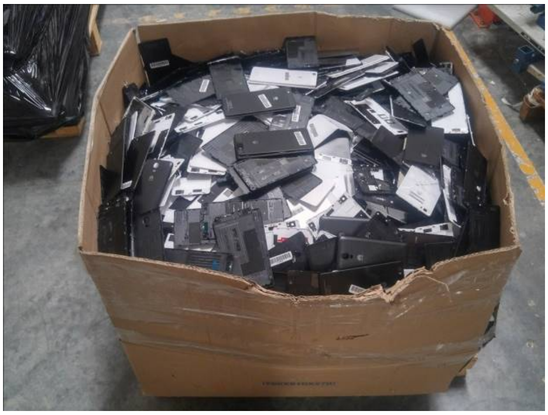


15. Scrapped Mobile Phone 3

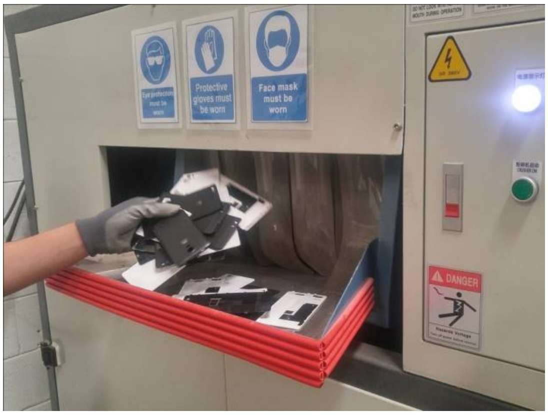


D. Shredding Process

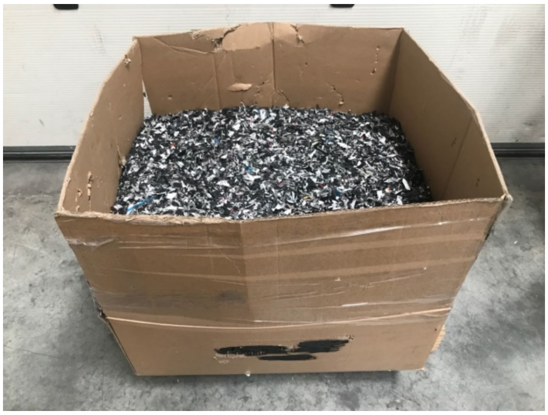
18. Back Cover Before Shredded



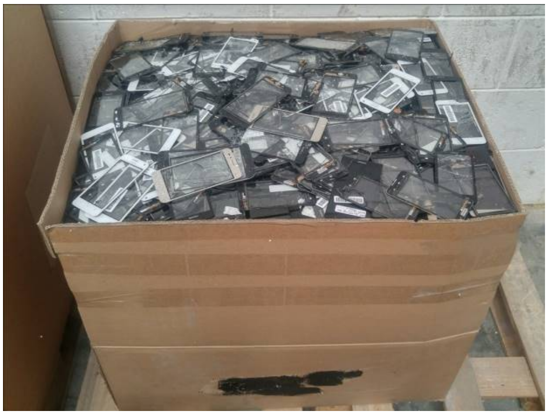
18. Shredding



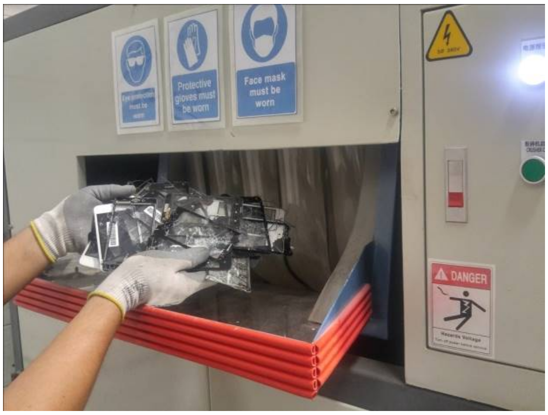
18. Over-All Shredded Back Cover



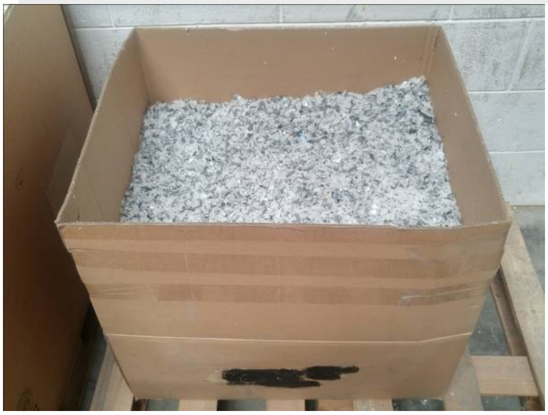
19. Glass Screen Before Shredded



19. Shredding

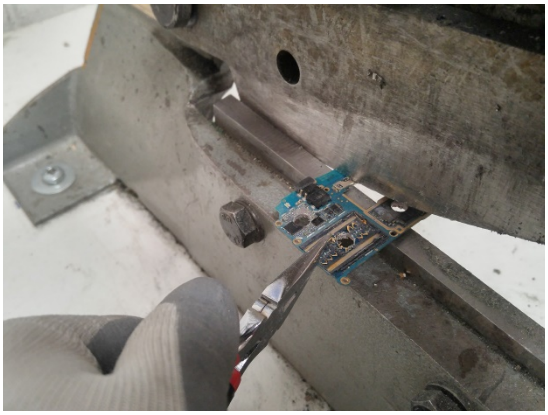


19. Over-All Shredded Glass Screen

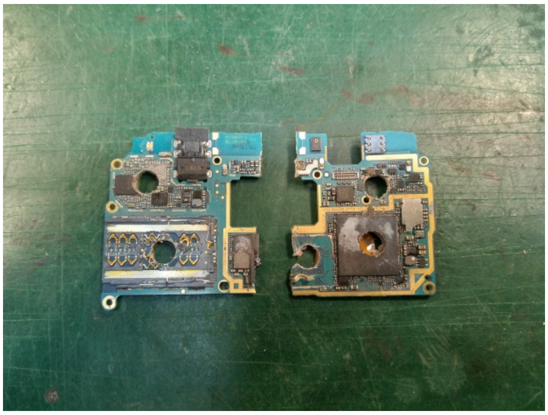


D. Shredding Process

26. Cutting



26. Scrapped PCB 4



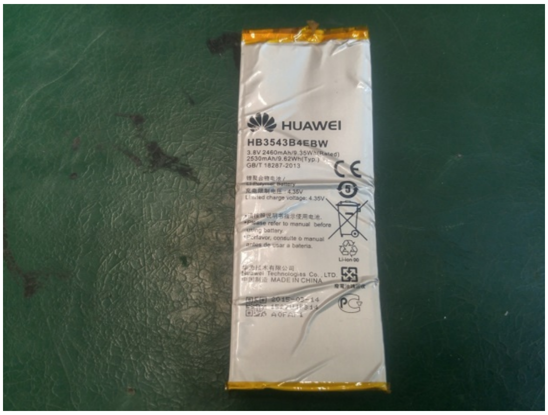
27. Over-All Scrapped PCB

28. Scrapped Materials Collection

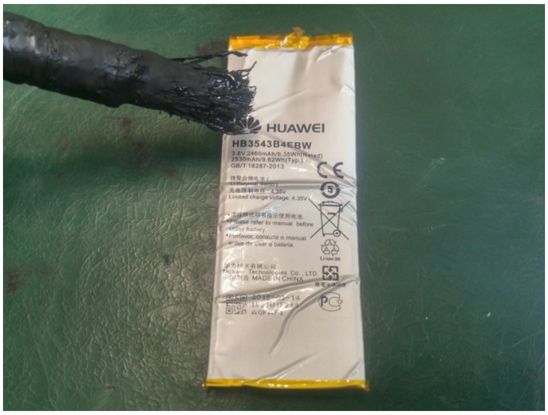
End of Report

E. Battery Packing Process

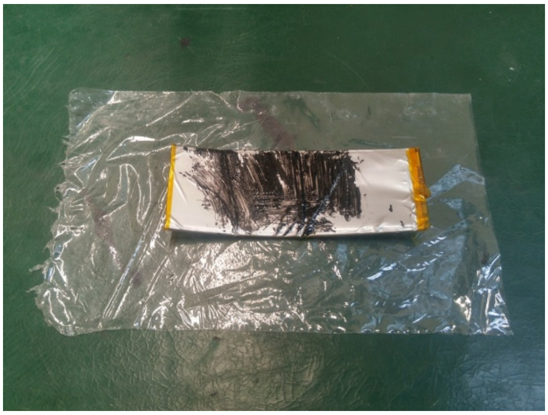
20. Battery 1 Before Scrapped



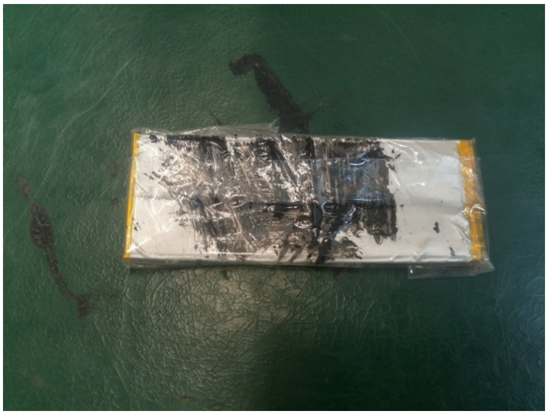
20. Painting Label



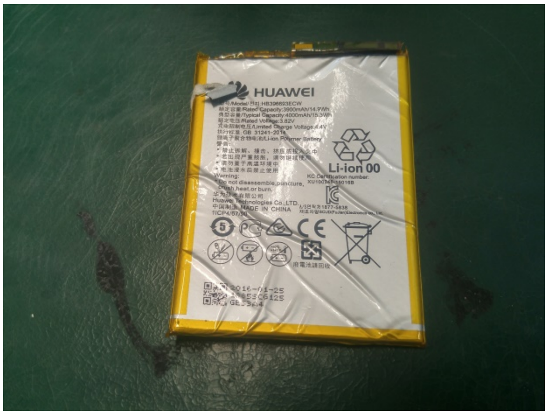
20. Wrapping



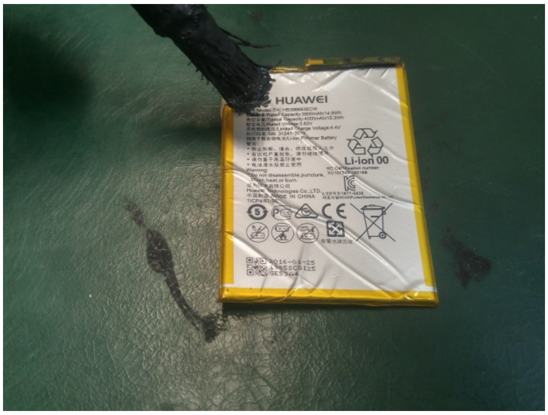
20. Scrapped Battery 1



21. Battery 3 Before Scrapped

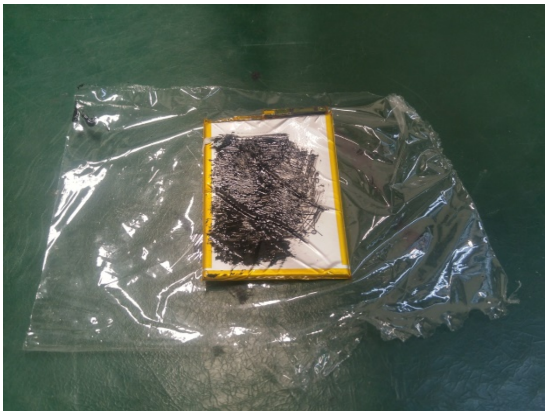


21. Painting Label

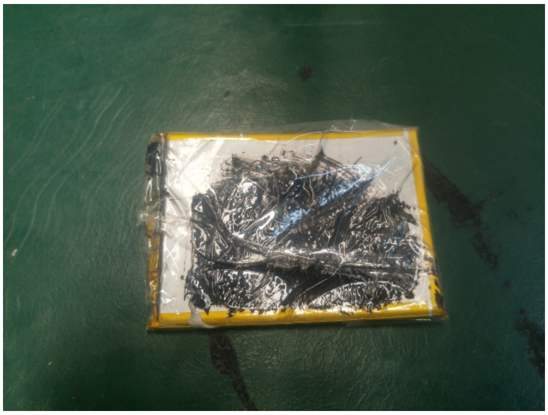


E. Battery Packing Process

21. Wrapping

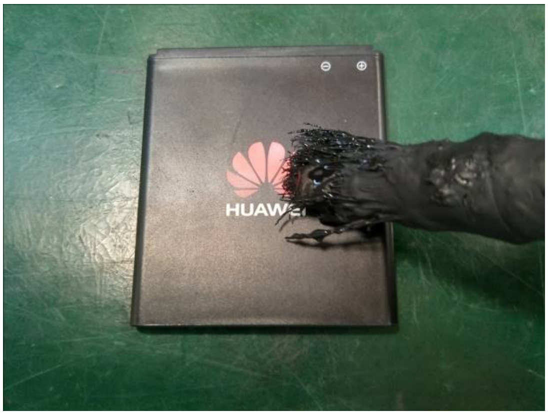


21. Scrapped Battery 2

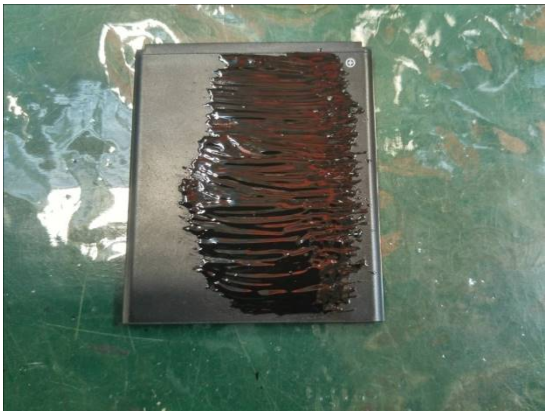


22. Battery 3 Before Scrapped

22. Painting Label



22. Wrapping



22. Scrapped Battery 3