

<b>Policy title</b>	<b>Enforcement Policy 2017</b>
Contact person	General Manager Legal & Compliance
Policy overview	<p>This policy:</p> <ul style="list-style-type: none"> <li>describes the Authority's approach to enforcing breaches of the Code by industry participants and the Authority</li> <li>outlines the Authority's enforcement options</li> <li>makes transparent the factors that the Authority will take into account when deciding which enforcement option to use.</li> </ul>
Approval authority	Chief Executive (exercising delegation to approve minor changes to policies)
Date approved	20 March 2017
Legal review	February 2017
Filesite reference	1039834-1

## Version control

Version number	Date	Author	Description (including Board reference if relevant)
1	20-03-17	Jillian	<p>Policy formed by amalgamating the following documents:</p> <ul style="list-style-type: none"> <li>Compliance Philosophy</li> <li>Operating Procedures for Processing Alleged Breaches of the Code</li> <li>Guidelines for Monitoring and Enforcing Alleged Breaches by the Authority</li> </ul> <p>Approved on 20-03-17 by Chief Executive exercising delegation to approve minor changes to policies.</p>

## Approvals

**CE**

1,039,819

CE approval WorkSite ref #

Ross Hill, General Manager  
Legal & Compliance  
**Policy Owner**

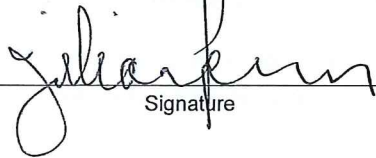


Signature

28.3.2017

Date

Jillian Penn, Legal Counsel  
**Policy Author**



Signature

27/3/2017

Date

## **Glossary of abbreviations and terms**

<b>Authority</b>	Electricity Authority
<b>Act</b>	Electricity Industry Act 2010
<b>Board</b>	Electricity Authority Board
<b>Committee</b>	Compliance Committee
<b>Code</b>	Electricity Industry Participation Code 2010
<b>Compliance database</b>	database
<b>participant</b>	industry participant
<b>Regulations</b>	Electricity Industry (Enforcement) Regulations 2010
<b>settlement</b>	settlement agreement



# Contents

<b>Glossary of abbreviations and terms</b>	<b>3</b>
<b>1. Purpose</b>	<b>7</b>
<b>2. The Authority's Prosecution Policy</b>	<b>7</b>
<b>3. Compliance philosophy</b>	<b>7</b>
<b>4. Case management</b>	<b>8</b>
<b>5. Quality review</b>	<b>8</b>
<b>6. Processing alleged breaches of the Code</b>	<b>9</b>
Reporting a breach of the Code	9
Processing notifications	10
Fact finding	11
Fact finding report to Committee	11
Criteria for recommendation	12
Compliance Committee decision	15
Additional decisions	15
Case study and precedent cases	15
Close the file	16
Conflicts	16
Further information required	17
<b>7. Investigation</b>	<b>17</b>
Notify alleged breaching party	17
Publicise investigation	17
Other participants join the investigation	18
Obligations on participants	18
Obligations on the investigator	19
Endeavour to effect a settlement of Code breaches	19
Draft settlement agreement	20
Settlement achieved	20
Recommendations to the Committee	22
Settlement not achieved	23
Committee options	24

	Compliance Committee decision	25
	Board decision	27
<b>8.</b>	<b>Monitoring and enforcing alleged breaches of the Code by the Authority</b>	<b>28</b>
	Introduction	28
	Separation of investigation and market operation service provider roles	28
	Independent audit of Authority’s investigation	29
	Decisions made by the Authority in relation to an alleged breach	29
<b>Appendix A</b>	<b>Flowchart of the Code breach process</b>	<b>31</b>
<b>Appendix B</b>	<b>Code breach assessment guidelines</b>	<b>33</b>
	Overview	33
	Alleged code breaches and assessment criteria	33
	Impact on security, consumers, and market	33
	Criteria matrix for assessing severity and overall impact of alleged breaches	33
<b>Appendix C</b>	<b>Code breach check sheet</b>	<b>35</b>
	Checklist for formal investigations	35
<b>Appendix D</b>	<b>Default dispute resolution process under Part 6 of the Code (Connection of Distributed Generation)</b>	<b>39</b>

# 1. Purpose

- 1.1 The Electricity Authority (Authority) has developed this policy to:
- (a) describe our approach to enforcing breaches of the Electricity Industry Participation Code 2010 (Code) by industry participants and the Authority
  - (b) outline our enforcement options
  - (c) make transparent the factors that we will take into account when deciding which enforcement option to use.
- 1.2 The body of this policy focuses in particular on the processes and requirements relating to how the Authority:
- (a) receives and processes an alleged breach of the Code
  - (b) investigates and enforces an alleged breach of the Code.
- 1.3 Appendices A to D of this policy set out:
- (a) a flowchart summarising the steps in the Code breach process (Appendix A)
  - (b) the Breach Assessment Guidelines for assessing the severity of an alleged breach of the Code (Appendix B)
  - (c) a Code breach checklist for formal investigations (Appendix C)
  - (d) the default dispute resolution process for resolving disputes under Part 6 of the Code (Connection of Distributed Generation) (Appendix D).
- 1.4 Unless otherwise stated in this policy, a reference to a regulation (eg, "regulation 11(1)") is a reference to a regulation from the Electricity Industry (Enforcement) Regulations 2010 (Regulations).

# 2. The Authority's Prosecution Policy

- 2.1 The Authority's *Prosecution Policy* sets out how the Authority exercises its discretion in monitoring, investigating, and enforcing compliance with the Electricity Industry Act 2010 (Act) and any regulations made under the Act. The *Prosecution Policy* is available at <https://www.ea.govt.nz/code-and-compliance/compliance/prosecution-policy/>

# 3. Compliance philosophy

- 3.1 The Authority's Compliance philosophy guides decision-making at every stage of the compliance process:

The Authority's Compliance philosophy is to encourage continuous improvement by industry participants in the effective, efficient, and reliable operation of the electricity industry for the long-term benefit of consumers.

In doing this, the Authority will:

- (a) allocate resources where they are most needed
- (b) fast track "minor" breaches
- (c) formally investigate more serious breaches
- (d) refer the more severe or complex cases to the Rulings Panel
- (e) seek evidence that industry participants are "learning" when things go wrong, including ensuring that mitigating actions are taken to correct the problem and avoid recurrence
- (f) encourage settlement agreements between parties
- (g) take a pragmatic approach
- (h) ensure a good compliance process is always followed.

## **4. Case management**

4.1 The Authority uses a compliance database (database) to manage breach cases and facilitate achievement of timeliness targets. Timeliness targets anticipate that cases will be reported to the Compliance Committee (Committee) within four months of receiving a breach allegation. The database is kept up to date and includes a date-stamped activity log.

4.2 All compliance related documentation is filed electronically in the Authority's *FileSite* document management system. Paper based files are not used.

## **5. Quality review**

5.1 All key documentation produced by the Compliance team (Compliance) in the compliance process is quality reviewed, including all reports published on the Authority's website.

5.2 Quality review consists of:

- (a) peer review, to check for clarity of language, consistency, technical accuracy and good process
- (b) legal review, to ensure the documents are legally sound.



- 5.3 All reports to the Committee include a statement of compliance that the Authority's quality standard and compliance case management procedures have been met.

## 6. Processing alleged breaches of the Code

- 6.1 This policy provides guidance regarding the Code breach assessment process. Nothing in this policy is intended to prescribe or restrict the power of the Authority to exercise discretion when making decisions. In making decisions, the Authority will take into account all relevant factors, and will act in accordance with all relevant legislation and natural justice.
- 6.2 This policy should not be used as a substitute for participants taking their own legal advice.

### Reporting a breach of the Code

- 6.3 If a participant believes on reasonable grounds that another participant has breached the Code, the participant must report the breach or possible breach to the Authority as soon as possible.<sup>1</sup>
- 6.4 All common quality and security breaches of parts 7, 8, 9, or 13 of the Code, or any related provision in part 17 of the Code, must be reported to the Authority as soon as practicable.<sup>2</sup>
- 6.5 The report must be in writing and specify:<sup>3</sup>
- (a) the participant that is alleged to have breached the Code (the alleged breaching party)
  - (b) the provision of the Code allegedly breached
  - (c) the circumstances relating to the alleged breach
  - (d) the date and time the alleged breach occurred.
- 6.6 Alleged breaches may be reported through the database. Access to the database is made available to participants by email request to [compliance@ea.govt.nz](mailto:compliance@ea.govt.nz). Service providers must also report breaches in daily and monthly reports. Breaches may also be reported by completing and emailing the breach report template (<http://www.ea.govt.nz/document/8697/download/act-code-regs/compliance/how-to-allege-a-code-breach/>) to [compliance@ea.govt.nz](mailto:compliance@ea.govt.nz).
- 6.7 Any person, other than a participant, who believes on reasonable grounds that a participant has breached the Code may report the alleged breach to the

---

<sup>1</sup> Regulation 8(1).

<sup>2</sup> Regulation 7(1).

<sup>3</sup> Regulations 7(2) and 8(2).

Authority.<sup>4</sup> The Authority may allege a breach of the Code on this basis, because the Authority is not a participant.

## Processing notifications

- 6.8 All notifications must be recorded in the database to enable their progress to be tracked, assist in the management of workflows, and facilitate statistical reports being produced.
- 6.9 When Compliance staff receive a report of an alleged breach, they must:
- (a) for older cases recently reported, check the date of the alleged breach and the date the alleged breach was discovered because, under section 52 of the Act, the Authority may not exercise its powers in relation to a breach or a possible breach of the Code if the breach:
    - (i) was discovered, or ought reasonably to have been discovered, more than three years before the exercise of the power; or
    - (ii) occurred more than 10 years before the exercise of the power.
  - (b) check that the circumstances and date and time of the breach have been provided
  - (c) check whether the breach has been reported only by another participant and, if so, Compliance sends a fact finding letter to the breaching participant
  - (d) check whether the alleged breach has been reported by another participant and the participant allegedly in breach and, if so, both notifications will be associated to one breach event
  - (e) create a breach event in the database and assign it to a Compliance staff member
  - (f) create the electronic worksite folder in WorkSite.
- 6.10 Alleged breach information will be stored in the:
- (a) database: breach notification, breach assessment, log of compliance activity on the case, decision on the case, recommendation, and a copy of the information from the report to the Committee on the case (all documents provided by participants relating to the case are sent to WorkSite)
  - (b) electronic WorkSite folder: all documentation and all emails including attachments and scanned handwritten notes.

---

<sup>4</sup> Regulation 9.

- 6.11 If the time limitations apply, Compliance must write to the reporting party explaining why the Authority has no power to act in relation to the alleged breach.
- 6.12 However, if the Authority has exercised a power in relation to the breach or possible breach, the time limitations do not apply.

## **Fact finding**

- 6.13 After receiving a report of an alleged breach, Compliance checks whether it has all the information necessary to make a recommendation to the Committee. If the information provided by the reporting party is insufficient, Compliance may request the reporting party or any other participant to provide further information.
- 6.14 Compliance must keep confidential all information provided or disclosed to it through the breach reporting process, except to the extent that disclosure is required to enable the Authority to carry out its obligations and duties under the Regulations or the Code or is otherwise compelled by law.<sup>5</sup>
- 6.15 If Compliance considers that the reporting party has incorrectly specified the provision of the Code allegedly being breached, Compliance must advise the reporting party of this and ask the party would like to correct the provision specified.<sup>6</sup>
- 6.16 If the Authority considers that a breach has not occurred, Compliance must advise the reporting party accordingly and seek a response.<sup>7</sup>

## **Fact finding report to Committee**

- 6.17 Compliance must prepare a report and recommendation to present to the Committee.
- 6.18 The report and recommendation to the Committee must include the following information:
- (a) whether Compliance considers there was a breach
  - (b) whether the alleged breach is admitted or denied
  - (c) the full circumstances surrounding the event
  - (d) the impact (actual and potential market, security, operational, consumer) and the rationale for this

---

<sup>5</sup> Regulation 10.

<sup>6</sup> It is important to consider the substance of the allegation and the circumstances of the alleged breach to identify the correct provision in the Code. The numbering may have changed or the reporting party may have identified the wrong part of the Code. If the reporting party agrees that an incorrect Code provision has been specified, the database must be updated with the correct Code provision.

<sup>7</sup> There may be no breach if, on the facts, the identified provision in the Code (or any other provision) does not apply, or an exemption was in place at the time the alleged breach occurred.

- (e) remedial measures to resolve the matter and prevent further instances of a similar breach
- (f) previous breaches by the same participant or relevant compliance benchmarks
- (g) other information that Compliance may consider relevant.

6.19 Compliance must evaluate the severity of the alleged breach against the criteria in the Breach Assessment Guidelines (Appendix B), which can be found in the database “severity” section, to determine:

- (a) whether to recommend that the Committee:
  - (i) decline to pursue the alleged breach under regulation 11(1) with or without warning; or
  - (ii) appoint an investigator to investigate the alleged breach under regulation 12; and
- (b) whether to use:
  - (i) the minor alleged breaches of the Code template; or
  - (ii) the memorandum on Code breach template.

6.20 The report must specify whether the breach was:

- (a) self-reported (identified and reported by the breaching participant); or
- (b) reported by another participant.

## Criteria for recommendation

### Decline to pursue

6.21 Compliance may recommend the Committee decline to take action on a reported alleged breach if:

- (a) the report relates to a matter that has been, or that should more properly be, dealt with by any other person
- (b) the reporting participant fails to establish a prima facie case for the breach (in the case of a Code breach under regulation 11(1)(b)) (no breach); or
- (c) the alleged breach does not warrant further action being taken (in the case of a Code breach under regulation 11(1)(c)). The basis for this recommendation may be that the alleged breach is:
  - (i) minor;
  - (ii) caused minimal, if any, potential or actual market, financial, operational, consumer, or security impact;

- (iii) was not part of a systemic problem;
- (iv) was not a deliberate intention to breach the Code; and/or
- (v) the breaching party has taken steps to mitigate the breach impact and prevent recurrence.

6.22 In making its recommendation, Compliance also considers previous breaches by the same participant or relevant compliance benchmarks.

### **Early closure report**

- 6.23 An alleged breach may be suitable to be included in an minor alleged breaches of the Code report if, in addition to meeting the 'decline to pursue' criteria, the alleged breach is:
- (a) straightforward, so that it can be grouped, described in a summary report and summarised in a one-page table;
  - (b) not an alleged breach of a provision of part 7, 8, 9, or 13 of the Code that is about common quality or security, or any related provision in part 17 of the Code;
  - (c) inadvertent;
  - (d) admitted; and/or
  - (e) corrective action has been taken by the alleged breaching party to mitigate the breach impact and prevent recurrence.

### **Full memorandum**

- 6.24 An alleged breach may be suitable for presentation in a full memorandum if the alleged breach:
- (a) has greater complexity than an 'minor' alleged breach, so that it cannot easily be summarised in one page
  - (b) has aspects of concern and is therefore more likely to be accompanied with a warning letter (see below)
  - (c) is of a provision of part 7, 8, 9, or 13 of the Code that is about common quality and security, or any related provision in part 17
  - (d) is an alleged breach in respect of which Compliance is recommending that an investigator is appointed
  - (e) has aspects that may lead to the Authority considering proposing changes to the Code or existing procedures.
- 6.25 Compliance should provide the following in the memorandum:

- (a) a recommendation, and the legal grounds on which the recommendation is being made (eg, if the recommendation is to decline to pursue, the memorandum must specify if it is being made under regulation 11(1)(a), (b), or (c)<sup>8</sup>
- (b) a rationale for the recommendation
- (c) an assessment of the circumstances
- (d) the provision(s) of the Code alleged to have been breached
- (e) analysis of the breach which may include:
  - (i) a statement of whether the provision is permissive or mandatory
  - (ii) whether Compliance considers the provision to have been breached
  - (iii) whether Compliance considers that a Code amendment should be proposed to clarify ambiguity or inconsistency of a particular Code provision.

## Investigation

6.26 Compliance may recommend that the Committee investigate an alleged breach:

- (a) if the alleged breach has significant actual or potential impact (market, operational, or security and/or has affected a number of participants);
- (b) if the alleged breach is likely to recur (there are a number of previous breaches, no reasonable steps have been put in place to mitigate the alleged breach, and/or the alleged breach is denied);
- (c) if the alleged breach has complex surrounding circumstances;
- (d) if the notifying party and the alleged breaching party differ significantly in their interpretation of the breaching event;
- (e) if there is significant uncertainty about the interpretation of the relevant Code provision;
- (f) the alleged breach could be best resolved through the investigation process;
- (g) if an incentive to change a participant's attitude towards compliance is needed; and/or
- (h) if a settlement, which would improve significantly the participant's compliance, is likely to be achieved.

---

<sup>8</sup> This promotes transparency in the Authority's decision making processes as the decision is communicated back to the participants.

## Compliance Committee decision

### Decline to pursue

- 6.27 If the Committee decides to take no further action on an alleged breach, Compliance informs the notifying party and the alleged breaching party:
- (a) that the Authority intends to do no more in relation to the matter
  - (b) the reasons for its decision.<sup>9</sup>
- 6.28 If the Committee decides to take no further action on a breach, Compliance informs the notifying party and the participant that the Committee expects the participant to complete any actions to prevent recurrence and to advise the Authority accordingly.

## Additional decisions

### Warning letter

- 6.29 In some instances the Committee may decide to issue a warning letter if the alleged breach does not warrant further investigation but the participant has a pattern of non-compliance or the alleged breach has higher actual or potential market / security / operational impact.
- 6.30 In some cases the Committee may decide to issue a strong warning to a participant. The strong warning letter is sent to the Chief Executive Officer and/or Chair of the Board of the breaching participant.
- 6.31 Warning letters are usually signed by the Chair of the Committee. However, in less severe cases, the Committee may decide that Compliance should sign the letter.
- 6.32 All warning letters request a response to the Committee.

## Case study and precedent cases

- 6.33 The Committee may decide to use an alleged breach case as a case study if, for example, the alleged breach raises issues common to several participants.
- 6.34 If possible, Compliance should publish the full circumstances of the alleged breach. A case study can name a participant only with the consent of the participant concerned. If a participant does not give its consent, Compliance must ensure that the case study does not include any information identifying the participant who has withheld consent.
- 6.35 Committee decisions are flagged in the database as 'precedent' if the decision involves:

---

<sup>9</sup> Regulation 11(2).

- (a) an important legal issue; or
- (b) a problem with the interpretation of the Code.

## Close the file

6.36 Once the Committee's decision is carried out, Compliance records the decision and any participant's actions to prevent recurrence that have not been completed, then closes the file.

## Appoint an investigator

6.37 If the Committee decides to take further action on an alleged breach, the Committee must appoint an investigator on a temporary basis.<sup>10</sup> In this case, the status of the alleged breach event in the database is set to 'investigation'.

6.38 The Authority may appoint as investigator any person who it thinks has the requisite skills and experience to carry out an investigation.<sup>11</sup>

6.39 In practice, the Compliance staff member responsible for the file is usually appointed as investigator.

6.40 In some cases an external person may be appointed as an investigator, or the investigator appointed may appoint an external person to provide advice or assistance.<sup>12</sup>

6.41 In these cases, the external person will be provided with:

- (a) material information regarding the alleged breach (including any submissions from the alleged breaching party and other parties)
- (b) a copy of this policy
- (c) ongoing guidance throughout the process by a member of the Compliance team.

## Conflicts

6.42 When appointing an investigator, the Authority must take reasonable steps to ensure that the appointed person is free of conflicts of interest in carrying out the investigation.<sup>13</sup>

6.43 If an investigator appoints an external person to provide advice or assistance, the investigator must take reasonable steps to ensure that the appointed person is free of conflicts of interest in carrying out the investigation.<sup>14</sup>

---

<sup>10</sup> Regulation 12.

<sup>11</sup> Regulation 13(1).

<sup>12</sup> Regulation 14(1).

<sup>13</sup> Regulation 13(4).



6.44 If any conflict of interest arises, it must be dealt with in accordance with the Authority's *Disclosure of Interests Policy*.

### **Further information required**

6.45 The Committee may require further information before it makes a decision.

6.46 Once Compliance has collected the required additional information, Compliance must present a further report to the Committee:

- (a) attaching the additional information
- (b) making a recommendation to the Committee taking into account the additional information.

## **7. Investigation**

7.1 The purpose of an investigation is to:

- (a) establish the facts surrounding the alleged breach
- (b) endeavour to effect a settlement.

### **Notify alleged breaching party**

7.2 The investigator must promptly notify the alleged breaching party of the allegations that are being investigated, using reasonable endeavours to give this notice within five working days of being appointed.<sup>15</sup> The investigator should use the *Notice to Breaching Party* template. The 'circumstances of alleged breach' must clearly specify the provision of the Code allegedly breached, drawing a link between the requirements of the Code and the actions in contravention of the Code, so that the alleged breaching party and the parties that potentially may join the investigation be able to understand the nature of the allegations.

7.3 For further guidance on preparing the regulation 16 notice, see the "Regulation 16 checklist".<sup>16</sup>

### **Publicise investigation**

7.4 Investigations of alleged Code breaches (with the exception of alleged breaches of Part 6 of the Code) are publicised.

7.5 At the same time as the investigator sends the regulation 16 notice, the investigator must publicise the information about the matter under investigation,

---

<sup>14</sup> Regulation 14(2).

<sup>15</sup> Regulation 16.

<sup>16</sup> Filesite 538338.

including the content of the regulation 16 notice.<sup>17</sup> This is referred to as the "regulation 17 notice".

- 7.6 The regulation 17 notice (or a link to it) is published:
- (a) on the Authority's website
  - (b) in the following Market Brief
  - (c) in the investigation section of the database.
- 7.7 Investigations that are publicised are given the status of "open for joining" in the database. Participants are also able to see all details and notices of the investigation online in the database.
- 7.8 Investigations that are not publicised are given the status of "draft" in the database and are not visible in the database to participants.

### **Other participants join the investigation**

- 7.9 Any participant who considers that it is affected by the matter under a publicised investigation and wishes to become a party to the investigation must notify the investigator within ten working days after publication of the regulation 17 notice.<sup>18</sup> Participants can join investigations using the database. Participants using this feature are automatically added as parties to the investigation.
- 7.10 After ten working days, the investigator should arrange for the website to be updated to move the investigation to 'in progress, now closed for parties to join' on the website and to list all parties who have joined the investigation. The investigation's status in the database is changed to "closed for joining".

### **Obligations on participants**

- 7.11 The participant allegedly in breach must respond to the allegation within ten working days of receipt of the formal notification.<sup>19</sup> The investigator may grant an extension, in writing, for the alleged breaching party to respond to the notice.<sup>20</sup> A reasonable request is usually considered positively.
- 7.12 If a party is not cooperative, the investigator may consider using the Authority's information gathering powers under section 46 of the Act. When using the Authority's information gathering powers, the investigator follows the principles and procedures set out in the Authority's *Guidelines for the use of Information Gathering Powers for Compliance Purposes* available at

---

<sup>17</sup> Regulation 17.

<sup>18</sup> Regulation 17(2).

<sup>19</sup> Regulation 16(4).

<sup>20</sup> Ibid.

<http://www.ea.govt.nz/code-and-compliance/compliance/compliance-education-and-information/>.

## Obligations on the investigator

- 7.13 The investigator must conduct an investigation of the facts surrounding the alleged breach.<sup>21</sup> The investigator, and a person appointed by the investigator under regulation 14, must keep a copy of all relevant documentation on file and keep all information disclosed to him or her confidential, unless disclosure is required under regulation 15(1). It is Compliance's practice to ask in the regulation 16 and 17 notices the parties, to whom the notices are sent, to identify any information provided or disclosed that they consider confidential.

## Endeavour to effect a settlement of Code breaches

- 7.14 An investigator must endeavour to effect a settlement between the parties within 30 working days after the regulation 16 notice, or any other longer period agreed in writing between the investigator and the party.<sup>22</sup> In endeavouring to effect a settlement, the investigator may use any process considered by the investigator after consultation with the parties.<sup>23</sup>
- 7.15 As a suggested first step, the investigator can collate the parties' settlement requirements and circulate those requirements for the parties' comment. To assist the parties with their settlement requirements, the investigator may share with them information available to him in relation to this investigation. If the information, or part of it, is considered confidential, the investigator must seek consent from the party that provided information initially before releasing it.
- 7.16 The investigator should direct the parties towards a settlement that the Committee is likely to approve.
- 7.17 The settlement requirements should be:
- (a) more than just agreeing to comply with the Code
  - (b) specific to the particular circumstances of the alleged breach (eg, setting out specific actions and/or improved processes to be implemented by the alleged breaching party within set time frames to ensure compliance)
  - (c) consistent with the Code (a settlement must not be contrary to the Code).
- 7.18 Settlements are not generally binding on the Authority.<sup>24</sup> However, settlements are generally binding on all participants.<sup>25</sup>

---

<sup>21</sup> Regulation 20.

<sup>22</sup> Regulation 22(1) and (2).

<sup>23</sup> Regulation 22(3).

<sup>24</sup> Regulation 24(4)(a) and regulation 18.

- 7.19 The investigator should advise the parties that the investigator would not recommend that the Committee approve a settlement which contained terms contrary to the above criteria.
- 7.20 It may be difficult to reach agreement where settlement requirements cannot be agreed and/or a party requests that the matter be referred to the Rulings Panel. However, even in such circumstances, the investigator is obliged to 'endeavour' to effect a settlement.

### **Draft settlement agreement**

- 7.21 Once the parties have agreed in principle to a set of settlement requirements, the investigator drafts a settlement agreement (settlement), specifying the details of any breach of the Code that is admitted by the participant, and recording the terms of the settlement.<sup>26</sup>
- 7.22 It is possible to achieve a settlement where the parties do not admit the alleged breaches. However, the investigator should obtain and record a clear statement from the allegedly breaching party whether they admit or deny the alleged breach.
- 7.23 The draft should then be circulated for the parties' feedback, either via a settlement meeting, by correspondence, or via the specific database feature.

### **Settlement achieved**

#### **Parties notify acceptance**

- 7.24 The parties must notify their acceptance of the terms of the Settlement in writing to the investigator.<sup>27</sup> Parties can submit their settlement requirements via the database. If a party does not want the Settlement, or any part of it, published, it must advise the investigator.
- 7.25 The investigator then makes a recommendation to the Committee in the investigator's report as to whether there are special circumstances that justify the non-publication of the settlement, or any part of it.<sup>28</sup> Strong reasons are required to justify non-publication.

---

<sup>25</sup> Under regulation 24(4) but subject to regulation 26.

<sup>26</sup> Regulation 24(1)(b). Follow: 'Templates' 'Electricity Authority' 'Legal' 'Settlement Agreement'.

<sup>27</sup> Regulation 24(2).

<sup>28</sup> Regulation 25(2).

## Settlement and report to Committee

- 7.26 The investigator must provide the Committee with a copy of the Settlement, a report under regulation 19, and a recommendation on whether the Authority should approve the settlement.<sup>29</sup>
- 7.27 A report must set out sufficient details to enable the Authority to decide whether a formal complaint on the matter should be made to the Rulings Panel.<sup>30</sup> To the extent that is reasonably practicable and appropriate to the circumstances applying to the report, the report must set out or specify the following:<sup>31</sup>
- (a) the **provision of the Code** allegedly breached and any supporting information to assist the Committee better understand the purpose of the provision
  - (b) the **industry participant** alleged to have breached the Code
  - (c) the **estimated date and time** the breach allegedly occurred
  - (d) any **relevant issues** raised by the industry participant alleged to be in breach in response to the allegations of breach
  - (e) any **comments** made to the investigator by any other person in response to relevant issues raised by the industry participant alleged to be in breach
  - (f) any **additional information** that the investigator considers relevant to the decision of the Rulings Panel as to how the matter may be dealt with by the Rulings Panel
  - (g) the investigator's assessment of the **impact of the conduct** alleged to constitute the breach on the other industry participants
  - (h) the investigator's assessment of the likelihood of the alleged breach recurring
  - (i) details of any similar situations previously dealt with by the Authority (or its predecessor) or the Rulings Panel, including any settlement approved by the Authority under regulation 24(4) (or by its predecessor under any equivalent regulation) in response to those situations (if known by the investigator)
  - (j) a copy of all correspondence with the investigator or Authority relating to the alleged breach.

---

<sup>29</sup> Regulation 24(3).

<sup>30</sup> Regulation 19(2).

<sup>31</sup> Regulations 24(3) and 19(3).

## Recommendations to the Committee

### Options

- 7.28 The Committee may:
- (a) approve the settlement under regulation 24(4)(a); or
  - (b) reject the settlement under regulation 24(4)(b).
- 7.29 If the Committee rejects the Settlement, it must decide whether to recommend that the Board lay a formal complaint with the Rulings Panel.<sup>32</sup>
- 7.30 If the Committee rejects the Settlement and decides that no formal complaint should be laid, it must:
- (a) direct that the investigation be discontinued;<sup>33</sup> or
  - (b) direct the investigator to further endeavour to effect a settlement.<sup>34</sup>
- 7.31 If the Committee directs that the investigation is discontinued, regulation 28 applies.
- 7.32 If the Committee directs the investigator to further endeavour to effect a settlement, regulations 22 to 26 apply again, except that the time referred to in regulation 22 is 15 working days from the date of the direction, and the investigator may not allow further time.<sup>35</sup>

### Criteria for suitable recommendations

- 7.33 The investigator may make one of the recommendations listed below if, in addition to consideration under the Breach Assessment Guidelines (Appendix B), the criteria set out below are met.

### Recommend that the Authority approve the settlement

- 7.34 This may be appropriate if:
- (a) the parties have agreed to an appropriate solution to resolve the alleged breach;
  - (b) the party allegedly in breach has admitted the breach; or
  - (c) the party allegedly in breach has already taken steps to resolve the matter and prevent recurrence of a similar incident.

---

<sup>32</sup> Regulation 27(1).

<sup>33</sup> Regulation 27(3)(a).

<sup>34</sup> Regulation 27(3)(b).

<sup>35</sup> Regulation 27(4).

### **Reject the settlement and direct the investigator to further endeavour to effect a settlement**

7.35 This may be appropriate where the parties would benefit from a further round of negotiation, with the benefit of a Committee decision, in order to reach a settlement that the Committee is likely to approve.

### **Reject the settlement and abandon the investigation**

7.36 This may be appropriate if:

- (a) a party denies an alleged breach contrary to the view of the investigator and/or other parties; or
- (b) the term(s) of the settlement are insufficient, for example, they do not fulfil the requirements set out in paragraph 7.17 above; or
- (c) a party denies an alleged breach contrary to the view of the investigator and/or other parties; or
- (d) the breach is not so serious as to warrant laying a formal complaint with the Rulings Panel.

### **Reject the settlement and recommend that the Board lay a formal complaint**

7.37 Consistent with the Authority's Compliance philosophy, a referral to the Rulings Panel is appropriate for cases which generally fall on the high end of the Breach Assessment Guidelines. In particular:

- (a) the alleged breach has significant impact (on consumers and/or other parties/market/operations);
- (b) the alleged breach was deliberate;
- (c) the alleged breaching party failed to take appropriate action to rectify the alleged breach upon learning of it;
- (d) the alleged breaching party obtained a significant benefit or advantage as a result of the alleged breach;
- (e) the alleged breaching party has a pattern of repeated or ongoing non-compliance; or
- (f) the matter is of sufficient importance requiring a decision from the Rulings Panel.

### **Settlement not achieved**

7.38 Settlement is not possible if:

- (a) no party joins the investigation, or joins but later withdraws;
- (b) the alleged breaching party does not respond to the allegation;

- (c) there are no settlement requirements; or
- (d) settlement cannot be agreed.<sup>36</sup>

7.39 The investigator provides a report to the Committee recommending whether a formal complaint should be laid.<sup>37</sup> This report must be provided within 30 working days of the investigator giving notice under regulation 16 (or any longer period that the investigator agrees in writing).<sup>38</sup>

7.40 The report:

- (a) contains the matters set out in paragraph 7.27;<sup>39</sup> and
- (b) describes why a settlement was not achieved, attaching the parties' settlement requirement table, where relevant.

7.41 The investigator must ensure that all parties to the investigation are given a copy of this report.<sup>40</sup> It is sent to the parties after the Committee has made its decision.

## Committee options

7.42 The Committee may:

- (a) decide to discontinue the investigation under regulation 21, 23, or 27; or
- (b) recommend the Board lay a formal complaint with the Rulings Panel under regulation 30(1).

## Criteria

### Decide that no formal complaint should be laid

7.43 A recommendation that no formal complaint should be laid may be appropriate if:

- (a) a breach generally falls at the low to medium end of the Breach Assessment Guidelines
- (b) sufficient steps have been taken to remedy and prevent recurrence of the alleged breach
- (c) during the course of the investigation the alleged breach has been revealed to have no or minimal market impact, or there has been no breach; and/or

---

<sup>36</sup> If settlement is not possible due to the latter two options, the investigator should ensure that this is recorded in writing by the parties to the investigation.

<sup>37</sup> Regulation 19.

<sup>38</sup> Regulation 23(1)(a).

<sup>39</sup> To the extent reasonably practicable and appropriate: see regulation 19(3).

<sup>40</sup> Regulations 28(b) and 30(3).



- (d) the alleged breach may be better resolved by granting an exemption or through changes to the Code.

### **Recommend that the Board lay a formal complaint**

7.44 See paragraph 7.37 for the criteria to follow when deciding whether to lay a complaint with the Rulings Panel.

## **Compliance Committee decision**

### **Settlement achieved**

#### **Approve the settlement**

7.45 If the Committee approves a settlement, the investigator must:

- (a) notify all parties that the Authority approved the settlement
- (b) publicise the decision and the settlement at <http://www.ea.govt.nz/code-and-compliance/compliance/decisions/investigations-closed-settlement-reached/><sup>41</sup> (the Authority may decide not to publish the decision, or any part of it, if the Authority considers that there are special circumstances that justify the non-publication)<sup>42</sup>
- (c) update the Settlement Register, record the settlement actions, and make a record of this being completed
- (d) when all the above steps are completed, close the file by choosing the "Investigation – Settlement" close code.

7.46 Settlements are not generally binding on the Authority.<sup>43</sup> However, settlements are generally binding on all of the parties to the settlement.<sup>44</sup>

#### **Reject the settlement and direct the investigator to further endeavour to effect a settlement**

7.47 If the Committee rejects the settlement and directs the investigator to further endeavour to effect a settlement, the investigator must:

---

<sup>41</sup> A suggested format is:

[Date of settlement]

The Authority has approved the following settlement agreed between [list parties] in respect of [admitted/alleged breach(es)] of the Electricity Industry Participation Code by [alleged breaching party]. The matter concerned [briefly summarise nature of the alleged breach]. [Link to settlement and any appendices to the settlement.]

<sup>42</sup> Regulation 25.

<sup>43</sup> Regulation 24(4)(a) and regulation 18.

<sup>44</sup> Under regulation 24(4) but subject to regulation 26.

- (a) prepare the "Notification of the Authority's decision pursuant to regulation 29(1)" and instruct the Website Administrator to publicise this notice at <http://www.ea.govt.nz/code-and-compliance/compliance/decisions/> (the Authority may decide not to publish the decision, or any part of it, if the Authority considers that there are special circumstances that justify the non-publication)<sup>45</sup>
- (b) invite the parties to review the rejected Settlement in light of the Committee's comments
- (c) follow regulations 22 to 26
- (d) endeavour to effect a settlement within 15 working days from the date of the direction (the investigator may not allow further time).<sup>46</sup>

### **Reject the settlement and discontinue the investigation**

7.48 If the Committee decides to reject the settlement and discontinue the investigation, the investigator must:<sup>47</sup>

- (a) inform the parties of the decision and that, under regulation 31, they may lay a formal complaint against the alleged breaching party if the parties have suffered a loss as a result of the alleged breach
- (b) prepare the "Notification of the Authority's decision pursuant to regulation 29(1)" and publicise this notice under "Decisions not to lay a formal complaint" at <http://www.ea.govt.nz/code-and-compliance/compliance/decisions/> (the Authority may decide not to publish the decision, or any part of it, if the Authority considers that there are special circumstances that justify the non-publication)<sup>48</sup>
- (c) close the file (with the "Investigation – No Settlement" close code).

7.49 If the Committee approves a recommendation to discontinue the investigation but also decides to issue a warning, the investigator (in addition to informing the parties and publicising the decision as set out in paragraph 7.48) must:

- (a) issue the written warning, signed by the Chair of the Committee, to the alleged breaching party
- (b) close the file (with the "Investigation – No Settlement-Warning") close code.

---

<sup>45</sup> Regulation 29(1) requires the Authority to publicise every decision made under regulation 27(1), together with reasons for the Authority's decision.

<sup>46</sup> Regulation 27(4).

<sup>47</sup> Regulation 28.

<sup>48</sup> Regulation 29(1) requires the Authority to publicise every decision made under regulation 27(1), together with reasons for the Authority's decision.

## **Recommend laying a formal complaint with the Rulings Panel**

7.50 If the Committee recommends that the Board lay a formal complaint with the Rulings Panel, the investigator and the GM Legal and Compliance prepare a report to the Board, on behalf of the Committee, seeking approval to lay a formal complaint.

## **No settlement possible**

7.51 Follow either paragraph 7.48 or 7.50 above (with necessary modifications) depending on whether the Committee decides to recommend the Board lays a formal complaint under regulation 30(1).

## **Defer making a decision**

7.52 The Committee may defer consideration of a recommendation (eg, to recommend to the Board that the alleged breaches be referred to the Rulings Panel). This decision may be made to provide an opportunity for discussion between the participant allegedly in breach and other parties and/or senior advisers at the Authority, in order to explore alternative options.

## **Board decision**

### **Lay a formal complaint**

7.53 If the Board agrees that a complaint should be laid with the Rulings Panel, the investigator must:

- (a) publicise a notice under regulation 29(1) "Decisions to lay a formal complaint with the Rulings Panel" on:  
<http://www.ea.govt.nz/Codeandregs/compliance/decisions#rulings> (the Authority may decide not to publish the decision, or any part of it, if the Authority considers that there are special circumstances that justify the non-publication)<sup>49</sup>
- (b) formulate the complaint<sup>50</sup>
- (c) obtain the GM's approval of the final documentation to be submitted to the Rulings Panel
- (d) submit to the Rulings Panel the complaint and the regulation 19 investigator's report,<sup>51</sup> using the following suggested wording:

---

<sup>49</sup> A suggested format is:

'Complaint # and date of notice, linking though to notice

Summary [eg, Admitted/denied breach of [rule [x] of the Electricity Industry Participation Code concerning the [describe nature and time of breach]. Investigation notified and publicised on [date]]'.

<sup>50</sup> Regulation 30(1).

<sup>51</sup> Regulation 30(2).

"Dear Rulings Panel Member

Please find attached a formal complaint referred to the Rulings Panel by the Electricity Authority in relation to [a breach/breaches] of the Electricity Industry Participation Code 2010 by [participant].

Attached to the complaint is the notification publicising the Authority's decision to lay the formal complaint with the Rulings Panel. The notification is also posted on the Authority's website at: <http://www.ea.govt.nz/code-and-compliance/rulings-panel/>  
Also attached to the complaint is a copy of the investigator's report.

[any other points to be noted, ie, attachments that cannot be emailed due to size, confidentiality requirements, etc]."

- (e) within five working days of the Board's decision, send copies of the complaint and report that were sent to the Rulings Panel, to the parties to the investigation
- (f) update the file with the "Rulings Panel" close code.

### **Not to lay a formal complaint**

7.54 If the Board decides not to lay a formal complaint, the process for implementing this decision is set out in paragraph 7.30 above.

## **8. Monitoring and enforcing alleged breaches of the Code by the Authority**

### **Introduction**

8.1 The steps the Authority must take to manage situations in which the Authority is required to monitor, investigate, and enforce possible breaches of the Code by the Authority are set out below. The purpose of the guidelines is to ensure that possible breaches and breaches of the Code by the Authority are dealt with in an impartial, fair, and transparent manner.

### **Separation of investigation and market operation service provider roles**

#### **Initial fact finding**

8.2 If the Authority becomes aware of a possible breach of the Code by the Authority, the Authority must conduct an initial fact finding exercise as if the possible breach was committed by any other participant.

8.3 If the Authority declines to take action on any report of an alleged breach in accordance with regulation 11, the Authority must publicise its reasons for declining to take action. This requirement goes beyond the requirements in the

Regulations, to ensure that decisions made about alleged breaches of the Code by the Authority are transparent.

- 8.4 If an interested participant is concerned about the process followed by the Authority in the initial fact finding exercise, the participant may request that the Authority's process is audited by an independent person. If such a request is made, the requirements set out at paragraphs 10.7 and 10.8 apply.

## **Investigation**

- 8.5 The Authority must ensure that any person appointed to investigate allegations of breaches of the Code under the Regulations is not in any way involved in the market operation service provider functions of the Authority. As set out in regulation 13, the Authority must take reasonable steps to ensure that the appointed person as an investigator is free of conflicts of interest in carrying out the investigation.
- 8.6 An investigator appointed by the Authority to investigate a possible breach of the Code by the Authority must declare to the Authority any potential conflict of interest as soon as he or she becomes aware of the conflict. This may occur when an investigator is unable to carry out the investigation in an independent manner. If there is such a conflict of interest, the Authority must appoint another investigator who is free of any conflicts of interest to investigate the alleged breach.

## **Independent audit of Authority's investigation**

- 8.7 To ensure that any investigation carried out by the Authority regarding a possible breach of the Code by the Authority is impartial, the investigation process must be audited by an independent person.
- 8.8 The investigation process must be certified to have been undertaken independently before the Authority makes a decision under regulations 21, 23, or 27. The Authority must publicise that certification when it publicises its decision under regulation 29.

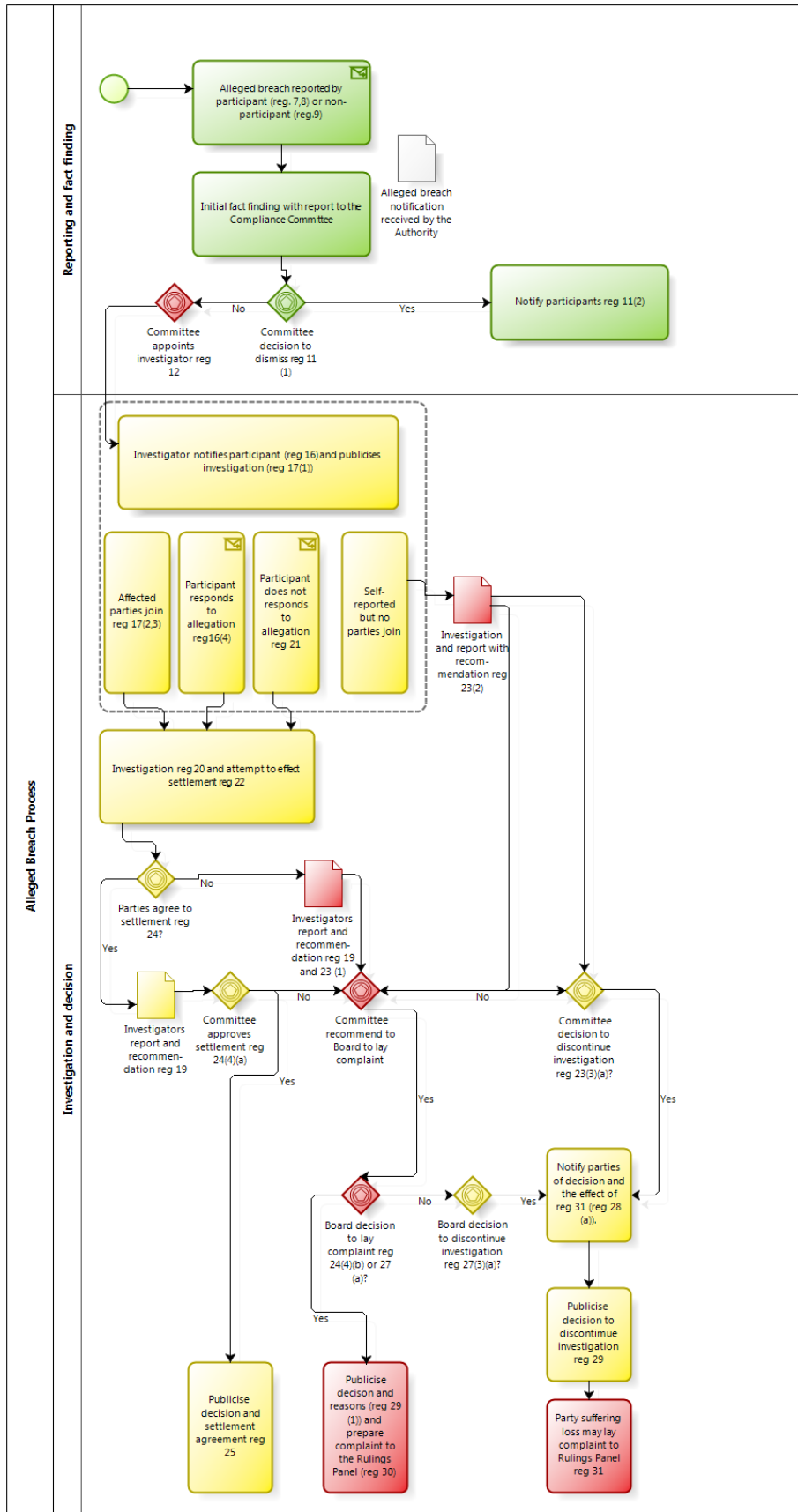
## **Decisions made by the Authority in relation to an alleged breach**

- 8.9 When making any decision under the Regulations in relation to an alleged breach of the Code by the Authority, the Authority must be mindful of its obligation to act in an impartial manner. The Authority must make such decisions as if the alleged breach was committed by any other participant.
- 8.10 To ensure transparency of decisions of the Authority in relation to alleged breaches of the Code, the Regulations require that the Authority publicise:
- (a) every decision, and reasons for the decision, made under regulations 21, 23, and 27
  - (b) terms of any settlement approved under regulation 24.

- 8.11 As set out above, if the Authority declines to take action on any report of an alleged breach of the Code by the Authority, the Authority must publicise its reasons for declining to take action.

## **Appendix A Flowchart of the Code breach process**

A.1 The Code breach process can be shown by the following flowchart:





# Appendix B Code breach assessment guidelines

## Overview

1. These guidelines set out the criteria that the Authority uses to assess the seriousness and overall impact of alleged breaches of the Code by participants. This assessment assists the Authority in its decisions on how individual alleged breaches are categorised and dealt with.
2. These guidelines are not prescriptive. They set out the factors the Authority will have regard to and consider when exercising its judgement.

## Alleged code breaches and assessment criteria

3. The Authority assesses each alleged breach against the criteria matrix set out below and then decides which category the alleged breach falls into and how it should be dealt with. These criteria are not exhaustive and additional factors, such as the participant's general compliance performance and the number of occasions in the past when the same clause has been breached by the participant may also be taken into account.

## Impact on security, consumers, and market

4. When making assessments about security impact, the Authority may consider the following additional factors:
  - a. the number of assets involved, and their importance to the system
  - b. deviation from normal operational parameters
  - c. probability of driving frequency out of the normal frequency band
  - d. extended reserve tripping or cascade failure.
5. When making assessments about consumer impact, the Authority may consider any relevant factors, eg, financial or operational.
6. Market impact may result in disruption of orderly trading or departure from generating and distributing energy at the lowest cost to the customers. Market impact in financial terms (actual or potential) needs to be put into context (eg, time, geographical extent, costs to clear the impact):

## Criteria matrix for assessing severity and overall impact of alleged breaches

7. The database screen (shown below) is populated in every case and the application determines the severity automatically. The investigator has the option to override the automatically generated result based on the investigator's judgement and discretion.

### Database screen for assessment

**Severity**

<b>Low</b>	<b>Medium</b>	<b>High</b>
<input type="radio"/> No or minimal security impact	<input type="radio"/> Local security impact	<input type="radio"/> Wide spread security impact
<input type="radio"/> No or minimal operational impact	<input type="radio"/> Moderate operational impact	<input type="radio"/> High operational impact
<input type="radio"/> No or minimal market impact	<input type="radio"/> Moderate market impact	<input type="radio"/> Significant to severe market impact
<input type="radio"/> No or minimal potential security impact	<input type="radio"/> Local potential security impact	<input type="radio"/> Wide spread potential security impact
<input type="radio"/> No or minimal potential operational impact	<input type="radio"/> Moderate potential operational impact	<input type="radio"/> High potential operational impact
<input type="radio"/> No or minimal potential market impact	<input type="radio"/> Moderate potential market impact	<input type="radio"/> Significant to severe potential market impact
<input type="radio"/> Inadvertent	<input type="radio"/> Careless	<input type="radio"/> Deliberate
<input type="radio"/> One off event	<input type="radio"/> Previous occurrences	<input type="radio"/> Recent previous occurrences
<input type="radio"/> Procedures in place	<input type="radio"/> Procedures/Processes require improvement	<input type="radio"/> Systemic – lack of procedures
<input type="radio"/> Full understanding	<input type="radio"/> Limited understanding	<input type="radio"/> Questionable understanding
<input type="radio"/> Low probability of recurrence	<input type="radio"/> Medium probability of recurrence	<input type="radio"/> High probability of recurrence
<input type="radio"/> Irregular activity	<input type="radio"/> Regular activity	<input type="radio"/> Continuous activity
<input type="radio"/> Short duration - minutes	<input type="radio"/> Medium duration - hours	<input type="radio"/> Long duration - days/weeks/months
<input type="radio"/> Low number of previous breaches	<input type="radio"/> Medium number of previous breaches	<input type="radio"/> High number of previous breaches

Severity   Override

Investigators perception of the severity

## Appendix C Code breach check sheet

### Checklist for formal investigations<sup>52</sup>

Investigation:

Investigator:

Completed	Action	Regulation	Peer review	Legal review
	Investigator appointed	12	n/a	n/a
	Notify participant in breach within 5 working days. <ul style="list-style-type: none"> <li>• Prepare notice</li> <li>• Notice emailed to participant.</li> </ul>	16		
	Publicise Investigation at same time as notifying under regulation 16. <ul style="list-style-type: none"> <li>• Prepare notice, place on website with regulation 16 notice.</li> <li>• Send link to Compliance email contacts list.</li> <li>• Provide copy to Communications for weekly update.</li> </ul>	17(1)		
	Participant alleged in breach responds within 10 working days.	16(4)		
	Participant alleged in breach requests extension to 10 working day response period. <ul style="list-style-type: none"> <li>• Investigator grants extension in writing.</li> </ul>	16(4)		
	Conduct an investigation of the facts.	20		
	Participant alleged in breach does not respond within the time allowed. <ul style="list-style-type: none"> <li>• Investigator must prepare report as soon as practicable that complies with regulation 19.</li> </ul> <p>Note: Although the participant has not responded, regulation 22 requires an investigator to effect a settlement on every matter under investigation.</p>	21(1)		

<sup>52</sup> Filesite 665466.

Completed	Action	Regulation	Peer review	Legal review
	<p>Participants affected may join investigation within 10 working days</p> <ul style="list-style-type: none"> <li>• Receive notifications of joining and provide acknowledgement.</li> </ul>	17(2)		
	<p>For self-reported breaches under regulation 7 if no other party joins the Investigation.</p> <ul style="list-style-type: none"> <li>• Investigator must prepare report as soon as practicable that complies with regulation 19.</li> </ul>	23(2)		
	<p>After 10 working days of notification</p> <ul style="list-style-type: none"> <li>• Move the notification on website to, "Investigations in progress - now closed for parties to join" page.</li> </ul>			
	<p>Endeavour to effect a settlement</p> <ul style="list-style-type: none"> <li>• Investigator provides investigation findings, participant's response to regulation 16 notice and requests settlement requirements. (Information provided to parties is subject to consent if marked confidential.)</li> </ul>	22		
	<p>Agree in writing with any party that settlement will take more than 30 working days.</p>	22		
	<p>Settlement not reached</p> <ul style="list-style-type: none"> <li>• Provide report that complies with regulation 19 and recommendation to Authority.</li> </ul>	23(1)		
	<p>Authority makes decision on report – decision to discontinue the Investigation.</p> <ul style="list-style-type: none"> <li>• Notify parties to the Investigation of the decision and of the effect of regulation 31.</li> <li>• Provide parties with a copy of the Investigator's report.</li> </ul>	23(3)(a)  28(a)  28(b)		
	<p>Authority makes decision on report – decision to lay a formal complaint.</p> <p>The Investigator:</p> <ul style="list-style-type: none"> <li>• Formulates formal complaint.</li> <li>• Submits complaint and copy of report to the Rulings Panel within 5 working days.</li> <li>• Provides a copy of the Complaint and the Investigator's report to all parties.</li> </ul>	23(3)(b)  30(1)(a) 30(1)(b) & 30(2) 30(3)		

Completed	Action	Regulation	Peer review	Legal review
	<ul style="list-style-type: none"> <li>Publicises the decision to lay a formal complaint. Decision on website, includes in weekly communication update.</li> </ul>	29(1)		
	<p>Settlement reached</p> <ul style="list-style-type: none"> <li>Must be in writing; and</li> <li>Specify the details of any admitted breach; and</li> <li>Record the terms of settlement.</li> <li>Parties notify acceptance of terms in writing.</li> <li>Investigator provides report that complies with regulation 19, copy of settlement and recommendation to Authority.</li> </ul>	24		
	<p>Authority approves settlement.</p> <ul style="list-style-type: none"> <li>Investigator publicises settlement by placing on website.</li> <li>Investigator removes Investigation from website section "Investigations in progress - now closed for parties to join".</li> </ul>	24(4)(a) 25(1)		
	<p>Authority rejects the settlement and decides to lay a formal complaint.</p> <p>The Investigator:</p> <ul style="list-style-type: none"> <li>Formulates formal complaint.</li> <li>Submits complaint and copy of report to the Rulings Panel within 5 working days.</li> <li>Provides a copy of the complaint and the Investigator's report to all parties.</li> </ul>	24(4)(b), 27  30(1)(a) 30(1)(b) & 30(2) 30(3)		
	<p>Authority rejects the settlement and decides to discontinue the Investigation.</p> <p>The Investigator:</p> <ul style="list-style-type: none"> <li>Notifies parties to the Investigation of the decision and of the effect of regulation 31.</li> <li>Provide parties with a copy of the Investigator's report.</li> <li>Publicises the decision to lay a formal complaint. Decision on website, includes in</li> </ul>	27(3)(a)   29(1)		

Completed	Action	Regulation	Peer review	Legal review
	<p>weekly communication update.</p> <ul style="list-style-type: none"> <li>Investigator removes Investigation from website section 'Investigations in progress - now closed for parties to join'.</li> </ul>			
	<p>Authority rejects the settlement and directs the Investigator to further effect a settlement.</p> <p>The Authority may decide not to publicise this decision.</p> <p>The Investigator:</p> <ul style="list-style-type: none"> <li>Publicises the decision it the unless the Authority decides not to under regulation 29(2).</li> <li>Advises parties to the investigation and further endeavours to effect a settlement.</li> <li>The settlement must be achieved within 15 days from the date of the direction.</li> <li>If a settlement is not achieved, the investigator prepares and provides a report to the Authority.</li> </ul>	<p>27(3)(b)</p> <p>29(2)</p> <p>27(4)</p> <p>27(4)</p> <p>23(1)</p>		

## Appendix D Default dispute resolution process under Part 6 of the Code (Connection of Distributed Generation)

- D.1 A complaint under clause 2(3) of Schedule 6.3 of the Code must be treated as if it were a notification given under the Regulations. Sections 53 to 62 of the Act and the Regulations (except regulations 5, 6, 7, 9, 17, 51 to 75, and subpart 2 of part 3) apply to the complaint.
- D.2 Once received by the Authority, a complaint is generally managed within the regular alleged breach process. With only two parties involved and due to the nature of these disputes, there are a few exceptions to this general rule. These are discussed below.

### Receive complaint and fact finding

- D.3 A distributed generator or a distributor may complain in writing about an alleged breach by the other of Part 6 of the Code to the Authority.<sup>53</sup>
- D.4 The complaint must be related to a dispute arising from any one of the following:<sup>54</sup>
- (a) an allegation that a party has breached any of the regulated terms that apply under clause 6.6(2); and
  - (b) an allegation that conditions specified by the distributor under clause 18 of Schedule 6.1 are not reasonably required; and
  - (c) an allegation that a party has not attempted to negotiate in good faith under clause 6 or clause 21 of Schedule 6.1; and
  - (d) an allegation that a party has breached any of the other provisions of Part 6 of the Code.
- D.5 The default dispute resolution process does not apply if the dispute between a distributed generator and a distributor:<sup>55</sup>
- (a) arises from an allegation that a party has breached any of the terms of a connection contract;
  - (b) arises from an allegation that a party has breached any of the extra terms referred to in clause 6.7(1) of the Code; or

---

<sup>53</sup> Clause 2(3) of Schedule 6.3 of the Code.

<sup>54</sup> Clause 6.8(1) of the Code.

<sup>55</sup> Clause 6.8(2) of the Code.

- (c) is one that the distributed generator and the distributor have agreed should be determined by any other agreed method (eg, under any dispute resolution scheme under section 95 of the Act).

D.6 The complaint should include:

- (a) a description of the dispute
- (b) a copy of the written notice given to the other party of the dispute
- (c) evidence of the good faith attempts taken with the other party to attempt to resolve the dispute.

D.7 The Compliance staff member should determine whether the complaint satisfies the requirements in paragraphs D.3 to D.6.

### **Differences to the breach process**

D.8 Only parties to the connection in question can complain.

D.9 No party, other than the distributor or distributed generator, can be party to the process at any stage.

D.10 The fact finding stage includes the facilitation of a settlement, or other mutually acceptable outcomes between the parties.